Guida a Ubuntu Server

Guida a Ubuntu Server

Sommario

Benvenuti nella *Guida a Ubuntu server*. Questa guida contiene informazioni su come installare e configurare diverse applicazioni server per Ubuntu a seconda delle proprie esigenze. È una guida passo-passo, orientata ai processi per configurare e personalizzare il sistema.

Riconoscimenti e licenza

Questo documento viene mantenuto dal gruppo documentazione di Ubuntu (https://wiki.ubuntu.com/DocumentationTeam). Un elenco dei collaboratori è riportato nel prosieguo.

Collaboratori a questo documento:

- Membri di *Ubuntu Documentation Project*[2]
- Membri di *Ubuntu Server Team*[3]
- Collaboratori di *Ubuntu Documentation Wiki*[4]
- Altri collaboratori possono essere trovati nella storia delle revisioni di *serverguide*[5] e *ubuntu-docs*[6]; linee di sviluppo Bazaar disponibili su Launchpad.

[1] http://creativecommons.org/licenses/by-sa/3.0/
[2] https://launchpad.net/~ubuntu-core-doc
[3] https://launchpad.net/~ubuntu-server
[4] https://help.ubuntu.com/community/
[5] https://code.launchpad.net/serverguide
[6] https://code.launchpad.net/ubuntu-docs

Indice

Lista delle tabelle

Capitolo 1. Introduzione

Benvenuti alla guida a *Ubuntu server*.

In questa guida è possibile trovare informazioni su come installare e configurare diversi applicativi server; è una guida passo-passo, orientata ai processi per configurare e personalizzare il proprio sistema.

This guide assumes you have a basic understanding of your Ubuntu system. Some installation details are covered in *Capitolo 2, Installazione [3]*, but if you need detailed instructions installing Ubuntu please refer to the *Ubuntu Installation Guide*[1].

Una versione HTML di questa guida è disponibile in rete presso il *sito web di Ubuntu*[2].

1 https://help.ubuntu.com/12.10/installation-guide/
2 https://help.ubuntu.com

1. Supporto

Esistono diverse forme di supporto per la Ubuntu Server Edition: supporto commerciale e dalla comunità. Il supporto commerciale è disponibile attraverso Canonical Ltd.: fornisce contratti di supporto a prezzi ragionevoli per postazione desktop o server. Per maggiori informazioni, consultare il *sito web di Canonical*[3].

Il supporto della comunità è fornito grazie all'impegno di singole persone, o di aziende, che desiderano rendere Ubuntu il migliore sistema operativo possibile. Il supporto viene erogato attraverso l'utilizzo di mailing list, canali IRC, forum, blog, wiki e altro. L'enorme quantità di informazioni disponibili può sembrare schiacciante, ma una valida interrogazione con un motore di ricerca può spesso fornire una risposta ai propri dubbi. Per maggiori informazioni, consultare la pagina *Ubuntu Support*[4].

[3] http://www.canonical.com/services/support
[4] http://www.ubuntu.com/support

Capitolo 2. Installazione

This chapter provides a quick overview of installing Ubuntu 12.10 Server Edition. For more detailed instructions, please refer to the *Ubuntu Installation Guide*[1].

[1] https://help.ubuntu.com/12.10/installation-guide/

1. Preparazione dell'installazione

Questa sezione spiega i diversi aspetti da considerare prima di avviare l'installazione.

1.1. Requisiti di sistema

Ubuntu 12.10 Server Edition supports three (3) major architectures: Intel x86, AMD64 and ARM. The table below lists recommended hardware specifications. Depending on your needs, you might manage with less than this. However, most users risk being frustrated if they ignore these suggestions.

Tabella 2.1. Requisiti minimi raccomandati

Tipo di installazione	CPU	RAM	Spazio disco fisso	
			Sistema di base	Installazione completa
Server (Standard)	1 gigahertz	512 megabytes	1 gigabyte	1.75 gigabytes
Server (Minimal)	300 megahertz	256 megabytes	700 megabytes	1.4 gigabytes

La Server Edition fornisce una base comune per tutte le tipologie di applicazioni server: ha una progettazione minimalista in grado di fornire una piattaforma per qualsiasi servizio desiderato come servizi di file e stampa, host web, email, ecc...

1.2. Differenze tra Server e Desktop

Ci sono alcune differenze fra la *Ubuntu Server Edition* e la *Ubuntu Desktop Edition*. È utile ricordare però che entrambe le edizioni utilizzano i repository apt, rendendo l'installazione di un'applicazione *server* sulla Desktop Edition facile come sulla Server Edition.

The differences between the two editions are the lack of an X window environment in the Server Edition and the installation process.

1.2.1. Differenze del kernel

Ubuntu version 10.10 and prior, actually had different kernels for the server and desktop editions. Ubuntu no longer has separate -server and -generic kernel flavors. These have been merged into a single -generic kernel flavor to help reduce the maintenance burden over the life of the release.

Usando una versione a 64-bit di Ubuntu su processori a 64-bit non si è limitati nello spazio di indirizzamento della memoria.

To see all kernel configuration options you can look through `/boot/config-3.5.0-server`. Also, *Linux Kernel in a Nutshell*[2] is a great resource on the options available.

[2] http://www.kroah.com/lkn/

1.3. Effettuare una copia di backup

- Prima di installare Ubuntu Server Edition è utile creare una copia di sicurezza di tutti i dati nel sistema. Per maggiori informazioni sulle opzioni di backup, consultare il *Capitolo 19, Backup [296]*.

  Se non è la prima volta che viene installato un sistema operativo nel computer, potrebbe essere necessario ripartizionare il disco fisso per creare spazio per l'installazione di Ubuntu.

  A ogni partizionamento del disco fisso è necessario essere preparati per eventuali perdite di dati causate da errori o da malfunzionamenti nel sistema di partizionamento. I programmi usati durante l'installazione sono sicuri e usati da molti anni, ma possono anche eseguire azioni distruttive.

2. Installare da CD

I passi di base per installare Ubuntu Server Edition dal CD sono uguali a quelli necessari per installare qualunque sistema operativo dal CD. Diversamente dalla *Desktop Edition*, la *Server Edition* non include un programma di installazione con interfaccia grafica: la Server Edition utilizza invece un processo basato su un menù a console

- Per prima cosa, scaricare e masterizzare il file ISO appropriato dal *sito web di Ubuntu*[3].
- Avviare il sistema dal CD-ROM.
- Al prompt dell'avvio verrà richiesto di selezionare una lingua.
- Nel menù principale di avvio sono presenti alcune opzioni aggiuntive per l'installazione di Ubuntu Server Edition: è possibile installare una versione di base, controllare l'eventuale presenza di difetti nel CD, controllare la RAM del sistema, effettuare l'avvio dal primo disco fisso o ripristinare un sistema danneggiato. La parte rimanente di questa sezione tratterà l'installazione di base di Ubuntu Server.
- Il programma d'installazione chiede quale lingua usare e quindi di selezionare la posizione.
- Inizia quindi il processo d'installazione con una richiesta relativa alla disposizione della tastiera: è possibile tentare un rilevamento automatico o selezionarla manualmente da un elenco.
- Il programma d'installazione rileva l'hardware e configura le impostazioni di rete utilizzando il servizio DHCP. Per non utilizzare questo servizio, alla schermata successiva scegliere «Indietro» e quindi scegliere l'opzione per configurare la rete manualmente.
- Vengono chiesti il nome host e il fuso orario.
- La disposizione del disco fisso si può scegliere fra diverse opzioni di configurazione; verrà quindi richiesto di specificare su quale disco effettuare l'installazione. Potrebbero essere richieste delle conferme prima di riscrivere la tabella delle partizioni o impostare il LVM, a seconda della disposizione del disco. Se viene scelto il LVM, verrà richiesta la dimensione della root del volume logico. Per maggiori informazioni sulle opzioni avanzate, consultare *Sezione 4, «Installazione avanzata» [10]*.
- Il sistema base Ubuntu viene quindi installato.
- Viene impostato un nuovo utente, che avrà un accesso *root* per mezzo dell'utilità sudo.
- Completate le impostazioni utente, verrà richiesto di cifrare la propria directory `home`.
- Il passo successivo nel processo di installazione consiste nel decidere come aggiornare il sistema. Sono disponibili tre opzioni:
  - *Nessun aggiornamento automatico*: richiede che un amministratore si colleghi al computer e installi manualmente gli aggiornamenti.
  - *Installare automaticamente gli aggiornamenti di sicurezza*: verrà installato il pacchetto unattended-upgrades, che installerà gli aggiornamenti di sicurezza senza l'intervento di un amministratore. Per maggiori informazioni, consultare *Sezione 5, «Aggiornamenti automatici» [29]*.

[3] http://www.ubuntu.com/download/server/download

- *Gestire il sistema con Landscape*: Landscape è un servizio a pagamento fornito da Canonical che consente di gestire diversi computer con Ubuntu installato. Per maggiori informazioni, consultare la *pagina web dedicata a Landscape*[4].
- Ora è possibile scegliere se installare o non installare diversi pacchetti per attività specifiche (tasks) (per maggiori informazioni, consultare *Sezione 2.1, «Pacchetti per attività specifiche» [7]*). È inoltre presente un'opzione per lanciare il programma aptitude per scegliere dei pacchetti specifici da installare. Per maggiori informazioni, consultare *Sezione 4, «Aptitude» [27]*.
- Infine, prima di riavviare, è necessario impostare l'orologio a UTC.

Se durante l'installazione non si è soddisfatti delle impostazioni predefinite, usare la funzione «Indietro» per visualizzare un menù d'installazione dettagliato che consente di modificare le impostazioni.

In qualsiasi momento dell'installazione è possibile leggere la guida fornita dal sistema, basta premere F1.

Once again, for detailed instructions see the *Ubuntu Installation Guide*[5].

2.1. Pacchetti per attività specifiche

Durante l'installazione della Server Edition è possibile installare dei pacchetti aggiuntivi, raggruppati per il tipo di servizio che forniscono.

- Server DNS: seleziona il server DNS BIND e la documentazione.
- Server LAMP: seleziona un server Linux/Apache/MySQL/PHP.
- Mail server: seleziona un gruppo di pacchetti utili per un sistema di server mail a scopo generale.
- Server OpenSSH: seleziona i pacchetti necessari per un server OpenSSH.
- Server PostgreSQL: seleziona i pacchetti client e server per il database PostreSQL.
- Server di stampa: configura il sistema come un server di stampa.
- Server file Samba: configura il sistema come server di file Samba, utile particolarmente all'interno di reti eterogenee, con sistemi Windows e Linux.
- Tomcat Java server: installa Apache Tomcat e le dipendenze necessarie.
- Virtual Machine host: comprende pacchetti necessari per la macchina virtuale KVM.
- Manual package selection: esegue aptitude, che consente di selezionare singolarmente i pacchetti.

L'installazione dei gruppi di pacchetti è effettuata con l'impiego dell'utilità tasksel. Una delle principali differenze tra Ubuntu (o Debian) e altre distribuzioni GNU/Linux è che un pacchetto, quando viene installato, è anche configurato con ragionevoli impostazioni predefinite, richiedendo talvolta informazioni addizionali. Allo stesso modo, installando un «task», i pacchetti vengono non solo installati, ma anche configurati per fornire un servizio pienamente integrato.

[4] http://www.canonical.com/projects/landscape
[5] https://help.ubuntu.com/12.10/installation-guide/

Una volta completata l'installazione, è possibile vedere un elenco dei «task» disponibili digitando il seguente comando:

```
tasksel --list-tasks
```

L'output elenca i «task» di altre distribuzioni basate su Ubuntu come Kubuntu ed Edubuntu. È comunque possibile invocare il comando **tasksel**, che presenta un menù con i diversi «task» disponibili.

Tramite l'opzione *--task-packages* è possibile visualizzare un elenco dei pacchetti installati con ogni «task». Per esempio, per elencare i pacchetti installati con *DNS Server* digitare:

```
tasksel --task-packages dns-server
```

L'output del comando dovrebbe essere:

```
bind9-doc
bind9utils
bind9
```

Se un «task» non viene installato durante il processo d'installazione, ma si decide per esempio di far funzionare il nuovo server LAMP anche come server DNS, è sufficiente inserire il CD d'installazione e digitare da un terminale:

```
sudo tasksel install dns-server
```

3. Avanzamento di versione

Ci sono diversi metodi per eseguire un avanzamento da un rilascio di Ubuntu a un altro. In questa sezione vengono presentati i metodi raccomandati.

3.1. do-release-upgrade

Il metodo di avanzamento raccomandato per la Server Edition è l'utilizzo dell'utilità do-release-upgrade, installata in modo predefinito come parte del pacchetto *update-manager-core* e priva di alcuna dipendenza grafica.

I sistemi basati su Debian possono ricorrere anche al comando **apt-get dist-upgrade**. L'uso di do-release-upgrade è comunque raccomandato in quanto è in grado di gestire le modifiche necessarie alla configurazione di sistema tra i rilasci.

Per avanzare a un nuovo rilascio, da un terminale digitare:

```
do-release-upgrade
```

È anche possibile usare do-release-upgrade per avanzare a una versione di sviluppo di Ubuntu. Per fare ciò, usare l'opzione *-d*:

```
do-release-upgrade -d
```

Avanzare a una versione di sviluppo *non* è consigliato in ambienti di produzione.

4. Installazione avanzata

4.1. RAID software

«RAID», Redundant Array of Independent Disks (*insieme ridondante di dischi indipendenti*), è un metodo che impiega più dischi per fornire diverse combinazioni fra aumento dell'affidabilità dei dati e, o in alternativa, l'aumento delle prestazioni I/O, a seconda del livello RAID utilizzato. RAID è implementato o a livello software (il sistema operativo è al corrente dell'esistenza di entrambi i dischi e li gestisce attivamente) o a livello hardware (uno speciale controller presenta al SO l'array come un singolo disco e gestisce tutti i dischi in maniera «invisibile»).

Il RAID software incluso nelle attuali versioni di Linux (e Ubuntu) è basato sul driver mdadm e funziona perfettamente, molto meglio di alcuni cosiddetti controller RAID hardware. In questa sezione viene spiegato come installare Ubuntu Server Edition utilizzando due partizioni RAID1 su due dischi fissi, uno utilizzato per */* e l'altro come *swap*.

4.1.1. Partizionamento

Seguire i passi dell'installazione fino a giungere a *Partizionamento dei dischi*, quindi:

1. Selezionare *Manuale* come metodo di partizionamento.
2. Selezionare il primo disco fisso e acconsentire alla domanda *Creare una nuova tabella delle partizioni sul dispositivo*.

   Ripetere questo passo per ogni disco da inserire nell'array RAID.
3. Selezionare lo *spazio libero* sul primo disco e quindi selezionare *Creare una nuova partizione*.
4. Selezionare la *Dimensione* della partizione: questa partizione sarà quella di *swap* e come regola generale, la dimensione della partizione di swap è solitamente il doppio della memoria RAM. Digitare la dimensione della partizione, scegliere *Primaria* e quindi *Inizio*.

   Una partizione di swap di dimensione doppia rispetto alla capacità RAM disponibile può non essere sempre consigliabile, specialmente nei sistemi con una grande quantità di RAM: il calcolo della partizione di swap nei server dipende fondamentalmente dal modo in cui sarà utilizzato il sistema.
5. Selezionare la riga in alto *Usare come:*: per impostazione predefinita è *File system ext4 con journaling*, modificarla in *volume fisico per il RAID* e poi *Impostazione della partizione completata*.
6. Per la partizione */*, selezionare *spazio libero* sul primo drive e quindi *Crea una nuova partizione*.
7. Utilizzare il restante spazio libero sul dispositivo e scegliere *Continua*, quindi *Primaria*.
8. Come per la partizione di swap, selezionare la riga in alto *Usare come:* e modificarla in *volume fisico per il RAID*. Selezionare anche la riga *Flag avviabile:* per cambiare il valore in *attivato*; scegliere quindi *Impostazione della partizione completata*.
9. Ripetere i passi dal 3 al numero 8 per gli altri dischi e partizioni.

4.1.2. Configurare RAID

Impostate le partizioni è quindi possibile configurare gli array:

1. Nella sezione di partizionamento dei dischi, selezionare *Configurare il software RAID*.
2. Selezione *Sì* per scrivere le modifiche sul disco.
3. Scegliere *Creare un device multidisk (MD)*.
4. Per questo esempio, selezionare *RAID1*. Nel caso si stia utilizzando una diversa configurazione, scegliere la tipologia adatta (RAID0 RAID1 RAID5).

Per poter usare il *RAID5* sono necessari almeno *tre* dischi. Per RAID0 oppure RAID1 solo *due*.

5. Inserire il numero dei dispositivi attivi (active), *2*, oppure il numero totale dei dischi disponibili per l'array, quindi selezionare *Continua*.
6. Inserire il numero dei dispositivi di scorta (spare), *0* come valore predefinito, quindi selezionare *Continua*.
7. Scegliere la partizione da usare: solitamente sda1, sdb1, sdc1, ecc... I numeri e le lettere solitamente corrispondono a diversi dischi fissi.

   Per la partizione di *swap* scegliere *sda1* e *sdb1*. Selezionare *Continua* per andare al passo successivo.
8. Ripetere i passi dal *tre* al *sette* per la partizione */* scegliendo *sda2* e *sdb2*.
9. Una volta completato tutto, selezionare *Terminare*.

4.1.3. Formattare

Dovrebbe essere visibile un elenco di dischi fissi e dispositivi RAID. Il passo successivo consiste nel formattare e impostare il punto di mount per i dispositivi RAID: tali dispositivi sono da considerare come dei normali dischi locali.

1. Selezionare *#1* nella partizione *Dispositivo RAID1 #0*.
2. Scegliere *Usato come:*, quindi *area di swap* e infine *Preparazione di questa partizione completata*.
3. Selezionare quindi *#1* nella partizione *Dispositivo RAID1 #1*.
4. Scegliere *Usato come:*, quindi *File system ext4 con journaling*.
5. Selezionare *Punto di mount* e scegliere */ - il file system root*. Modificare se necessario le altre opzioni e selezionare *Preparazione di questa partizione completata*.
6. Selezionare *Terminare il partizionamento e scrivere i cambiamenti sul disco*.

Se è stato scelto di posizionare la partizione di root nell'array RAID, il programma di installazione chiederà se avviare il sistema in modalità *degraded*. Per maggiori informazioni, consultare *Sezione 4.1.4, «RAID degraded» [12]*.

Il processo di installazione continuerà normalmente.

4.1.4. RAID degraded

Durante l'arco di vita di un computer si potrebbero verificare dei danni ai dischi. Quando si verifica un'eventualità come questa, usando il RAID software, il sistema operativo abilita la modalità *degraded* per l'array.

Se l'array è degradato («degraded») a causa di dati rovinati, il sistema operativo, in modo predefinito, si avvierà in *initramfs* dopo 30 secondi. Una volta avviato, è possibile, entro 15 secondi, continuare il normale avvio o tentare un ripristino manuale. L'avvio in initramfs potrebbe non essere consigliato, soprattutto se si opera sul computer da remoto. Avviare il sistema in un array «degraded» può essere svolto in diversi modi:

- L'utilità dpkg-reconfigure può essere usata per configurare il comportamento predefinito e durante l'elaborazione verranno poste delle domande relative a impostazioni addizionali per l'array come monitoraggio, avvisi via email, ecc... Per riconfigurare mdadm, digitare il seguente comando:

  ```
  sudo dpkg-reconfigure mdadm
  ```

- Il processo **dpkg-reconfigure mdadm** modificherà il file di configurazione `/etc/initramfs-tools/conf.d/mdadm`. Tale file presenta il vantaggio di pre-configurare il comportamento del sistema e può essere modificato a mano:

  ```
  BOOT_DEGRADED=true
  ```


  Il file di configurazione può essere scavalcato utilizzando un argomento per il kernel.

- È possibile avviare il sistema in un array «degraded» utilizzando anche un argomento per il kernel:
  - Durante l'avvio del computer, premere **Maiusc** per aprire il menù Grub.
  - Premere **e** per modificare le opzioni di comando del kernel.
  - Premere il tasto freccia **giù** per evidenziare il kernel.
  - Aggiungere *bootdegraded=true* alla fine della riga.
  - Premere **Ctrl**+**x** per avviare il sistema.

Una volta avviato il sistema, è possibile riparare l'array (consultare *Sezione 4.1.5, «Manutenzione RAID» [12]*) o copiare i dati importanti in un altro computer.

4.1.5. Manutenzione RAID

L'utilità mdadm può essere usata per visualizzare lo stato dell'array, aggiungere un disco all'array, rimuovere dischi, ecc...

- Per visualizzare lo stato di un array, da un terminale digitare:

```
sudo mdadm -D /dev/md0
```

L'opzione *-D* indica a mdadm di stampare informazioni *dettagliate* riguardo il device `/dev/md0`. Sostituire `/dev/md0` con il device RAID appropriato.

- Per visualizzare lo stato di un disco in un array:

```
sudo mdadm -E /dev/sda1
```

L'output è molto simile al comando **mdadm -D**, regolare `/dev/sda1` per ogni disco.

- Se un disco si rompe e deve essere rimosso da un array:

```
sudo mdadm --remove /dev/md0 /dev/sda1
```

Modificare `/dev/md0` e `/dev/sda1` con il device e il disco RAID appropriati.

- Per aggiungere un nuovo disco:

```
sudo mdadm --add /dev/md0 /dev/sda1
```

Qualche volta può succedere che un disco imposti il suo stato come *difettoso* («faulty»), anche se non presenta alcun malfunzionamento hardware. Può essere utile in questi casi rimuovere e aggiungere il disco all'array: verrà così nuovamente sincronizzato con l'array. Se il disco non riesce a sincronizzarsi con l'array, può indicare che il dispositivo sia effettivamente difettoso.

Il file `/proc/mdstat` contiene anche informazioni utili riguardo i device RAID del sistema:

```
cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sda1[0] sdb1[1]
      10016384 blocks [2/2] [UU]

unused devices: <none>
```

Il seguente comando è utile per controllare lo stato di un drive di sincronizzazione:

```
watch -n1 cat /proc/mdstat
```

Premere *Ctrl+C* per fermare il comando watch.

Se è necessario sostituire un disco difettoso, una volta sostituito e sincronizzato, è necessario reinstallare grub. Per installare grub nel nuovo disco, procedere come segue:

```
sudo grub-install /dev/md0
```

Sostituire `/dev/md0` con il nome dell'array appropriato.

4.1.6. Risorse

L'argomento degli array RAID è molto complesso e vasto poiché sono disponibili molti modi diversi di configurare un array RAID. Per maggiori informazioni, consultare i seguenti collegamenti:

- *Documentazione online riguardo RAID*[6].
- *Software RAID HOWTO*[7]
- *Managing RAID on Linux*[8]

4.2. Logical Volume Manager (LVM)

Logical Volume Manger, o *LVM*, consente agli amministratori di creare volumi *logici* da uno o più dischi fissi. I volumi LVM possono essere creati sia sulle partizioni RAID software sia sulle partizioni normali presenti su un singolo disco. I volumi possono essere estesi, garantendo un'alta flessibilità al sistema nel caso cambino le necessità.

4.2.1. Panoramica

Purtroppo, la potenza e la flessibilità di LVM, comportano maggiori complicazioni. Prima di tutto è quindi necessario introdurre la terminologia adatta.

- *Volume fisico (PV - Phisical Volume):* il disco fisso, la partizione di un disco o la partizione RAID software formattati come LVM.
- *Gruppo di volumi (VG - Volume Group):*è formato da uno o più volumi fisici; un VG può essere esteso aggiungendo ulteriori PV. Un VG è come un disco fisso virtuale, dal quale sono ricavati uno o più volumi logici.
- *Volume logico (LV - Logical Volume):* è simile a una partizione in un sistema non-LVM; un LV può essere formattato con il file system prescelto (EXT3, XFS, JFS, etc) ed è quindi disponibile per il montaggio e la memorizzazione dei dati.

4.2.2. Installazione

Come esempio, in questa sezione, viene descritto come installare Ubuntu Server Edition con `/srv` montato come volume LVM. Durante l'installazione un solo volume fisico (PV) farà parte del gruppo di volumi (VG). Un altro PV verrà aggiunto dopo l'installazione come dimostrazione delle funzionalità di estensione di un VG.

Sono disponibili diverse opzioni per l'installazione LVM, *Guidato - usare l'intero disco e impostare LVM* consente di assegnare una parte dello spazio disponibile a LVM, *Guidato - usare l'intero disco e impostare LVM cifrato* o *manuale*. Attualmente l'unico metodo per configurare un sistema affinché utilizzi sia partizioni LVM che normali durante l'installazione è quello manuale.

1. Seguire i passi dell'installazione fino a giungere a *Partizionamento dei dischi*, quindi:

---

[6] https://help.ubuntu.com/community/Installation#raid
[7] http://www.faqs.org/docs/Linux-HOWTO/Software-RAID-HOWTO.html
[8] http://oreilly.com/catalog/9781565927308/

2. Alla finestra *Partizionamento dei dischi* scegliere *Manuale*.
3. Selezionare il disco fisso e nella schermata successiva scegliere confermare *Creare una nuova tabella delle partizioni sul dispositivo*.
4. Creare le partizioni */boot*, *swap* e */* con il file system di propria scelta.
5. Per la partizione */srv* LVM, creare una nuova partizione *Logica* e modificare *Usato come* in *volume fisico per LVM*, quindi selezionare *Preparazione di questa partizione completata*.
6. Selezionare *Configurare il Logical Volume Manager* in alto e scegliere *Sì* per scrivere le modifiche sul disco.
7. Per il *Passo di configurazione di LVM* nella schermata successiva, scegliere *Creare gruppi di volumi*. Inserire un nome per il VG come *vg01* o qualche cosa più descrittivo. Fatto ciò, selezionare la partizione configurata per LVM e scegliere *Continua*.
8. Sempre nella schermata *Passo di configurazione di LVM*, selezionare *Creare volume logico*, selezionare il gruppo di volumi appena creato e inserire un nome per il nuovo LV, per esempio *srv* dato che verrà utilizzato come punto di mount per quella partizione. Scegliere la dimensione, che in questo caso può essere l'intera partizione dato che è possibile estenderla o ridurla, scegliere *Termina* per tornare alla schermata *Partizionamento dei dischi*.
9. Ora aggiungere il file system al nuovo LVM. Selezionare la partizione *LVM VG vg01, LV srv*, o in base al nome inserito, e scegliere *Usato come*. Impostare un file system selezionando */srv* come punto di mount e una volta completato, selezionare *Preparazione di questa partizione completata*.
10. Infine, selezionare *Terminare il partizionamento e scrivere i cambiamenti sul disco*, confermare le modifiche e continuare l'installazione.

Per visualizzare informazioni riguardo LVM sono disponibili diverse utilità:

- *pvdisplay:* visualizza informazioni riguardo i volumi fisici.
- *vgdisplay*: visualizza informazioni riguardo i gruppi di volumi.
- *lvdisplay:* visualizza informazioni riguardo i volumi logici.

4.2.3. Estendere i gruppi di volumi

Continuando con *srv* come esempio di un volume LVM, questa sezione spiega come aggiungere un secondo disco fisso, creare un volume fisico (PV), aggiungerlo al gruppo di volumi (VG), estendere il volume logico `srv` e infine estendere il file system. Questo esempio presume che sia stato aggiunto un secondo disco fisso al sistema, che verrà chiamato `/dev/sdb`; l'intero disco verrà usato come volume fisico (è possibile scegliere di creare partizioni e usarle come differenti volumi fisici).

Assicurarsi che non esista già un `/dev/sdb` prima di eseguire i seguenti comandi: se questi vengono eseguiti in un disco non vuoto, si potrebbe causare la perdita di dati.

1. Creare il volume fisico. In un terminale digitare:

```
sudo pvcreate /dev/sdb
```

2. Estendere il gruppo di volumi (VG):

```
sudo vgextend vg01 /dev/sdb
```

3. Usare vgdisplay per trovare gli extent fisici (PE) liberi (PE/dimensione = dimensione da allocare). In questo esempio viene considerata una dimensione di 511 PE (equivalenti a 2GB con una dimensione di PE di 4MB) e viene utilizzato tutto lo spazio libero. Utilizzare i PE in base alle proprie disponibilità.

   Il volume logico (LV) può essere esteso in diversi modi. In questo esempio viene considerato il caso di utilizzo del PE per estendere il LV:

```
sudo lvextend /dev/vg01/srv -l +511
```

   L'opzione *-l* consente di estendere il LV attraverso l'uso di PE. L'opzione *-L* invece, consente di estendere il LV utilizzando megabyte, gigabyte, terabyte, ecc...

4. Sebbene sia possibile *espandere* un file system ext3 o ext4 senza prima smontarlo, è comunque consigliabile smontarlo e controllare il file system, in modo da non fare pasticci allorquando sia necessario ridurre un volume logico (in tal caso il preliminare smontaggio è obbligatorio).

   I seguenti comandi sono pensati per un file system *ext3* o *ext4*. Se si sta utilizzando un altro file system potrebbero essere disponibili altri programmi.

```
sudo umount /srv
sudo e2fsck -f /dev/vg01/srv
```

   L'opzione *-f* di e2fsck forza il controllo anche se il file system sembra non avere problemi.

5. Infine, ridimensionare il file system:

```
sudo resize2fs /dev/vg01/srv
```

6. Montare la partizione e controllarne la dimensione.

```
mount /dev/vg01/srv /srv && df -h /srv
```

4.2.4. Risorse

- Consultare la *documentazione online riguardo LVM*[9].
- Per maggiori informazioni, consultare *LVM HOWTO*[10].
- Un ottimo articolo presente su linuxdevcenter.com è *Managing Disk Space with LVM*[11].

[9] https://help.ubuntu.com/community/Installation#lvm
[10] http://tldp.org/HOWTO/LVM-HOWTO/index.html
[11] http://www.linuxdevcenter.com/pub/a/linux/2006/04/27/managing-disk-space-with-lvm.html

- For more information on fdisk see the *fdisk man page*[12].

[12] http://manpages.ubuntu.com/manpages/quantal/en/man8/fdisk.8.html

5. Scaricamento del kernel in seguito a un crash (Kernel Crash Dump)

5.1. Introduzione

Un Kernel Crash Dump si riferisce a una porzione del contenuto della memoria volatile (RAM) che viene copiato nel disco ogni volta che viene interrotta l'esecuzione del kernel. I seguenti eventi possono causare un'interruzione del kernel:

- Kernel Panic
- Interrupt non mascherabile (Non Maskable Interrupts - NMI)
- Machine Check Exceptions (MCE)
- Errore hardware
- Intervento manuale

Per alcuni di tali eventi (panic, NMI) il kernel reagirà automaticamente innescando il meccanismo di scaricamento per mezzo di *kexec*, in altre situazioni è necessario un intervento manuale per conservare il contenuto della memoria. Ogni volta che si verifica uno degli eventi sopra menzionati, è importante scoprirne la causa, per evitare che si ripeta: questa può essere determinata esaminando il contenuto della memoria copiato.

5.2. Meccanismo del kernel crash dump.

Quando si verifica un kernel panic, il kernel dipende dal meccanismo *kexec* per un suo rapido riavvio in una sezione della memoria preassegnata durante l'avvio (come verrà spiegato in seguito). Questo consente di lasciare intatta l'area di memoria esistente per copiarne senza problemi il contenuto nel sistema di archiviazione.

5.3. Installazione

L'utilità kernel crash dump viene installata con il seguente comando:

```
sudo apt-get install linux-crashdump
```

È necessario un riavvio.

5.4. Configurazione

Non è necessaria nessuna ulteriore configurazione per abilitare la procedura di scaricamento del kernel.

5.5. Verifica

Per confermare l'abilitazione del meccanismo di scaricamento del kernel, occorre effettuare alcune verifiche. Per prima cosa, confermare che sia presente il parametro di avvio *crashkernel* (nota: La riga che segue è stata divisa in due per adattarla al formato di questo documento):

```
cat /proc/cmdline
```

```
BOOT_IMAGE=/vmlinuz-3.2.0-17-server root=/dev/mapper/PreciseS-root ro
 crashkernel=384M-2G:64M,2G-:128M
```

Il parametro *crashkernel* ha la seguente sintassi:

```
crashkernel=<range1>:<size1>[,<range2>:<size2>,...][@offset]
    range=start-[end] 'start' is inclusive and 'end' is exclusive.
```

Pertanto, per il parametro crashkernel trovato in `/proc/cmdline` si dovrebbe ottenere:

```
crashkernel=384M-2G:64M,2G-:128M
```

Il suddetto valore significa:

- se la RAM è inferiore a 384M, non verrà riservato nulla (questo è il caso «ripristino»)
- se la dimensione della RAM è compresa tra 386M e 2G (esclusiva), verrano riservati 64M
- se la dimensione della RAM è superiore a 2G, verranno riservati 128M

Occorre quindi verificare che il kernel abbia riservato l'area di memoria richiesta per effettuare il kdump del kernel, eseguendo:

```
dmesg | grep -i crash
```

```
...
[ 0.000000] Reserving 64MB of memory at 800MB for crashkernel (System RAM: 1023MB)
```

5.6. Collaudo del meccanismo di crash dump

Il collaudo del meccanismo del crash dump comporta *un riavvio del sistema*: in determinate situazioni, questo può causare una perdita di dati, se il sistema sta eseguendo un grosso carico di lavoro. Se è necessario collaudare il meccanismo, assicurarsi che il sistema sia inattivo o con un carico di lavoro molto leggero.

Verificare che il meccanismo *SysRQ* sia abilitato esaminando il valore del parametro del kernel `/proc/sys/kernel/sysrq`:

```
cat /proc/sys/kernel/sysrq
```

Se viene restituito il valore *0*, la caratteristica è disabilitata: abilitarla con il seguente comando:

```
sudo sysctl -w kernel.sysrq=1
```

Fatto questo, occorre diventare utente root, perchè non è sufficiente usare solo il comando **sudo**; come utente *root*, digitare il comando **echo c > /proc/sysrq-trigger**. Se si sta usando una connessione di rete, si verrà disconnessi dal sistema: ciò avviene in quanto è meglio effettuare il test essendo connessi alla console di sistema, perché si ha il vantaggio di rendere visibile il processo di scaricamento del kernel.

Un tipico output del test dovrebbe essere simile a quanto segue:

```
sudo -s
[sudo] password for ubuntu:
# echo c > /proc/sysrq-trigger
[ 31.659002] SysRq : Trigger a crash
[ 31.659749] BUG: unable to handle kernel NULL pointer dereference at (null)
[ 31.662668] IP: [<ffffffff8139f166>] sysrq_handle_crash+0x16/0x20
[ 31.662668] PGD 3bfb9067 PUD 368a7067 PMD 0
[ 31.662668] Oops: 0002 [#1] SMP
[ 31.662668] CPU 1
....
```

La parte rimanente dell'output è stata troncata, ma il sistema dovrebbe riavviarsi e da qualche parte nel log dovrebbe apparire la seguente riga:

```
Begin: Saving vmcore from kernel crash ...
```

; una volta completato il processo, il sistema si riavvia nella normale modalità operativa. Il file di scaricamento del kernel crash è nella directory `/var/crash`:

```
ls /var/crash
linux-image-3.0.0-12-server.0.crash
```

5.7. Risorse

Kernel Crash Dump è un argomento molto vasto che richiede una buona conoscenza del kernel di Linux; per maggiori informazioni, consultare:

- *Documentazione di Kdump kernel*[13].
- *The crash tool*[15].[14]
- *Analyzing Linux Kernel Crash*[16] (Basato su Fedora, fornisce comunque una buona spiegazione dello scaricamento del kernel).

[13] http://www.kernel.org/doc/Documentation/kdump/kdump.txt
[15] http://people.redhat.com/~anderson
[14] http://people.redhat.com/~anderson/
[16] http://www.dedoimedo.com/computers/crash-analyze.html

Capitolo 3. Gestione dei pacchetti

Ubuntu dispone di un completo servizio di gestione dei pacchetti per l'installazione, l'aggiornamento, la configurazione e la rimozione del software. Oltre a fornire accesso a più di 35000 pacchetti software per il proprio computer Ubuntu, il sistema di gestione dei pacchetti è in grado di gestire le risorse per la risoluzione delle dipendenze e di verificare l'esistenza di aggiornamenti.

Per l'interazione con il sistema di gestione dei pacchetti di Ubuntu sono disponibili diversi strumenti, a partire da semplici utilità a riga di comando che possono essere usate con facilità da amministratori di sistema per attività automatizzate, fino a interfacce grafiche semplici da usare per chi si è avvicinato da poco a Ubuntu.

1. Introduzione

Il sistema di gestione dei pacchetti di Ubuntu è derivato dallo stesso sistema usato dalla distribuzione Debian GNU/Linux. I file di pacchetto contengono tutti i file, i meta-dati e le istruzioni necessari per implementare sui sistemi Ubuntu una particolare funzionalità o un'applicazione software.

Di solito, i file dei pacchetti Debian presentano l'estensione «.deb» e risiedono nei *repository*, che sono delle collezioni di pacchetti memorizzate su diversi supporti, come un disco CD-ROM, o in rete. I pacchetti sono normalmente in formato binario precompilato: per questo l'installazione è veloce e non richiede la compilazione del software.

Molti pacchetti sfruttano il concetto delle *dipendenze*: dei pacchetti aggiuntivi richiesti dal pacchetto principale che si sta installando per poter funzionare correttamente. Per esempio, il pacchetto di sintesi vocale Festival dipende dal pacchetto libasound2, che fornisce la libreria audio ALSA necessaria per la riproduzione audio. Affinché festival possa funzionare, è necessario installare sia il programma che tutte le sue dipendenze. Gli strumenti di gestione del software in Ubuntu svolgono questa operazione automaticamente.

2. dpkg

dpkg è un gestore di pacchetti per i sistemi basati su *Debian*. È in grado di installare, rimuovere e generare i pacchetti, ma diversamente da altri sistemi di gestione dei pacchetti non può scaricare e installare automaticamente i pacchetti e le loro dipendenze. Questa sezione spiega come usare dpkg per la gestione locale di pacchetti installati:

- Per elencare tutti i pacchetti installati nel sistema, da un terminale digitare:

```
dpkg -l
```

- In base a quanti pacchetto sono installati nel sistema, questo comando può generare molto output. È comunque possibile passare l'output attraverso una pipe all'applicazione grep per vedere se un particolare pacchetto è installato o meno:

```
dpkg -l | grep apache2
```

  Sostituire *apache2* con il nome di un qualsiasi altro pacchetto, parte del nome o qualsiasi altra espressione regolare.

- Per elencare i file installati da un pacchetto, in questo caso ufw, digitare:

```
dpkg -L ufw
```

- Se non si è sicuri di quale pacchetto abbia installato un file, usare il comando dpkg -S. Per esempio:

```
dpkg -S /etc/host.conf
base-files: /etc/host.conf
```

  L'output mostra che `/etc/host.conf` appartiene al pacchetto base-files.

Molti file sono generati automaticamente durante il processo di installazione del pacchetto e, benché siano nel file system, il comando **dpkg -S** potrebbe non sapere a quale pacchetto appartengono.

- Per installare un file *.deb* locale, digitare:

```
sudo dpkg -i zip_3.0-4_i386.deb
```

  Modificare `zip_3.0-4_i386.deb` con il nome del file .deb da installare.

- Per disinstallare un pacchetto:

```
sudo dpkg -r zip
```

Disinstallare i pacchetti usando dpkg, nella maggior parte dei casi, *NOT* è raccomandato. È meglio usare un gestore di pacchetti in grado di gestire le dipendenze per assicurarsi che il sistema permanga sempre in uno stato consistente. Per esempio, usando **dpkg -r**

zip, è possibile rimuovere il pacchetto zip, ma qualsiasi pacchetto che vi dipende resterà installato e potrebbe non funzionare correttamente.

Per le ulteriori opzioni di dpkg, consultare la pagina di manuale: **man dpkg**.

3. Apt-Get

Il comando apt-get è un potente strumento a riga di comando usato per operare con l'*Advanced Packaging Tool* (APT) di Ubuntu al fine di eseguire operazioni come l'installazione di nuovi pacchetti software, l'aggiornamento dei pacchetti software esistenti, l'aggiornamento dell'indice dell'elenco dei pacchetti e persino l'avanzamento di versione dell'intero sistema Ubuntu.

Essendo un semplice strumento da riga di comando, apt-get presenta agli amministratori di sistema numerosi vantaggi rispetto ad altri strumenti di gestione dei pacchetti disponibili in Ubuntu. Alcuni di questi vantaggi sono la facilità d'utilizzo mediante semplici connessioni via terminale (SSH) e la possibilità di essere usato in script di amministrazione del sistema, magari automatizzati attraverso l'utilità di pianificazione cron.

Alcuni esempi di utilizzo tipico dell'utilità apt-get:

- **Installare un pacchetto**: l'installazione di pacchetti usando lo strumento apt-get è molto semplice. Per esempio, per installare lo scanner di rete nmap, digitare il seguente comando:

  ```
  sudo apt-get install nmap
  ```

- **Rimuovere un pacchetto**: la rimozione di uno o più pacchetti è altrettanto semplice e immediata. Per rimuovere il pacchetto installato nell'esempio precedente, digitare il seguente comando:

  ```
  sudo apt-get remove nmap
  ```


  Pacchetti multipli: è possibile specificare più di un pacchetto da installare o rimuovere, separati da spazi.

  Aggiungere l'opzione *--purge* ad **apt-get remove** fa in modo che vengano rimossi anche i file di configurazione del pacchetto. Usare questa opzione con cautela se non è ciò che si vuole.

- **Aggiornare l'indice dei pacchetti**: l'indice dei pacchetti di APT è essenzialmente un database dei pacchetti disponibili nei repository definiti nel file `/etc/apt/sources.list` e nella directory `/etc/apt/sources.list.d`. Per aggiornare l'elenco locale dei pacchetti con i cambiamenti apportati di recente nei repository, digitare il seguente comando:

  ```
  sudo apt-get update
  ```

- **Aggiornare i pacchetti**: versioni aggiornate dei pacchetti installati possono essere disponibili attraverso i repository dei pacchetti (per esempio per aggiornamenti di sicurezza). Per aggiornare il proprio sistema è necessario, prima di tutto, aggiornare l'indice dei pacchetti come spiegato sopra, quindi digitare:

  ```
  sudo apt-get upgrade
  ```

  Per informazioni sull'avanzamento a un nuovo rilascio di Ubuntu, consultare *Sezione 3, «Avanzamento di versione» [9]*.

Le azioni del comando apt-get, come l'installazione o la rimozione di pacchetti, vengono registrate nel file di registro /var/log/dpkg.log.

Per ulteriori informazioni sull'utilizzo di APT, consultare il dettagliato *Manuale utente di Debian APT*[1] o digitare:

```
apt-get help
```

[1] http://www.debian.org/doc/user-manuals#apt-howto

4. Aptitude

Lanciare Aptitude da riga di comando, con nessuna opzione, fornisce un'interfaccia testuale basata su menù per il sistema *Advanced Packaging Tool* (APT). Molte delle tipiche funzioni di gestione dei pacchetti, come l'installazione, la rimozione e l'aggiornamento, possono essere effettuate in Aptitude con dei comandi mappati su un solo tasto, solitamente delle lettere minuscole.

Aptitude è indicato in un ambiente non grafico per assicurare il corretto funzionamento dei comandi. È possibile avviare l'interfaccia basata su menù di Aptitude come normale utente eseguendo il seguente comando al prompt del terminale:

```
sudo aptitude
```

All'avvio di Aptitude, viene mostrata una barra dei menù nella parte superiore dello schermo e due riquadri sotto tale barra. Il riquadro superiore contiene delle categorie di pacchetto, come *Nuovi Pacchetti* e *Pacchetti non installati*. Il riquadro inferiore contiene le informazioni relative ai pacchetti e alle categorie di pacchetto.

Usare Aptitude per la gestione dei pacchetti è relativamente chiaro e l'interfaccia utente rende le operazioni comuni semplici da eseguire. Di seguito vengono presentati alcuni esempi di funzioni comuni della gestione dei pacchetti con Aptitude:

- **Installare pacchetti**: per installare un pacchetto, localizzare il pacchetto attraverso la categoria di pacchetto *«Pacchetti non installati»*, usando i tasti freccia sulla tastiera e il tasto **Invio**, in modo da evidenziare il pacchetto da installare. Premere quindi il tasto **+**: la voce relativa al pacchetto assume una colorazione *verde*, per indicare che è stato contrassegnato per l'installazione. Premere quindi il tasto **g** per ricapitolare le operazioni su pacchetti. Premendo nuovamente **g**, viene richiesto di acquisire i privilegi di amministrazione per completare l'installazione. Premere quindi **Invio** per mostrare un prompt *«Password:»*. Inserire la propria password utente per diventare root. Infine, premendo **g** ancora una volta, viene richiesto se scaricare il pacchetto. Premere **Invio** al prompt *Continua*: viene avviato lo scaricamento e l'installazione del pacchetto.
- **Rimuovere pacchetti**: per rimuovere un pacchetto, localizzare il pacchetto attraverso la categoria di pacchetto *Pacchetti installati*, usando i tasti freccia sulla tastiera e il tasto **Invio**, in modo da evidenziare il pacchetto da rimuovere. Premere quindi il tasto **-**: la voce relativa al pacchetto assume una colorazione *rosa*, per indicare che è stato contrassegnato per la rimozione. Premere quindi il tasto **g** per ricapitolare le operazioni sui pacchetti. Premendo nuovamente **g**, viene richiesto di acquisire i privilegi di amministrazione per completare la rimozione. Premere quindi **Invio** per mostrare un prompt *«Password:»*. Inserire la propria password utente per diventare root. Infine, premere **g** ancora una volta e quindi **Invio** al prompt *Continua*: viene avviata la rimozione del pacchetto.
- **Aggiornare l'indice dei pacchetti**: per aggiornare l'indice dei pacchetti è sufficiente premere il tasto **u** e verrà richiesto di diventare amministratori per completare l'aggiornamento. Premendo **Invio** viene presentata la richiesta della *password*. Inserire la password del proprio utente per

assumere i privilegi di amministratore: l'aggiornamento dell'indice dei pacchetti verrà avviato. Premere **Invio** al prompt *OK* quando appare la finestra di dialogo per scaricare quanto necessario al completamento del processo.

- **Aggiornare i pacchetti**: per aggiornare i pacchetti, eseguire l'aggiornamento dell'indice dei pacchetti come spiegato precedentemente, quindi premere il tasto **u** per selezionare tutti i pacchetti con aggiornamenti. Adesso premere **g** per avere un sommario delle azioni possibili sui pacchetti. Premere nuovamente **g** per assumere i privilegi di amministratore per completare l'installazione. Premere **Invio** e inserire la *password:*. Infine premere **g** ancora una volta per la richiesta di scaricare i pacchetti. Premere **Invio** al prompt *Continua* e l'aggiornamento dei pacchetti inizierà.

La prima colonna delle informazioni mostrate nell'elenco dei pacchetti nel riquadro superiore, indica l'attuale stato del pacchetto, utilizzando le seguenti chiavi per descrivere lo stato del pacchetto:

- **i**: pacchetto installato
- **c**: pacchetto non installato, ma nel sistema è rimasta traccia della configurazione del pacchetto
- **p**: rimosso completamente dal sistema
- **v**: pacchetto virtuale
- **B**: pacchetto non integro
- **u**: file decompressi, ma pacchetto non ancora configurato
- **C**: configurato in parte. La configurazione è fallita e necessita di essere corretta
- **H**: installato parzialmente. La rimozione è fallita e necessita di essere sistemata

Per chiudere Aptitude, è sufficiente premere il tasto **q** e confermare l'uscita. Sono disponibili molte altre funzioni dal menù di Aptitude, premendo il tasto **F10**.

4.1. Riga di comando Aptitude

Aptitude può anche essere utilizzato come strumento da riga di comando, simile ad apt-get. Per installare il pacchetto nmap con tutte le necessarie dipendenze, come nell'esempio di apt-get, usare il seguente comando:

```
sudo aptitude install nmap
```

Per rimuovere lo stesso pacchetto, usare il comando:

```
sudo aptitude remove nmap
```

Consultare le pagine man per ulteriori dettagli sulle opzioni della riga di comando di Aptitude.

5. Aggiornamenti automatici

Il pacchetto unattended-upgrades può essere usato per installare automaticamente gli aggiornamenti e può essere configurato per aggiornare tutti i pacchetti o installare solamente gli aggiornamenti di sicurezza. Per prima cosa, installare il pacchetto digitando:

```
sudo apt-get install unattended-upgrades
```

Per configurare unattended-upgrades, aprire il file `/etc/apt/apt.conf.d/50unattended-upgrades` e modificare quanto segue secondo le proprie esigenze:

```
Unattended-Upgrade::Allowed-Origins {
        "Ubuntu quantal-security";
//      "Ubuntu quantal-updates";
};
```

Alcuni pacchetti possono essere inseriti nella *blacklist* per non aggiornarli mai. Per inserire un pacchetto nella blacklist, aggiungerlo all'elenco:

```
Unattended-Upgrade::Package-Blacklist {
//      "vim";
//      "libc6";
//      "libc6-dev";
//      "libc6-i686";
};
```

I doppi slash («//») servono come commento; tutto quello che segue "//" non verrà valutato.

Per abilitare gli aggiornamenti automatici, modificare `/etc/apt/apt.conf.d/10periodic` e impostare le appropriate opzioni di configrazione di apt:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

La configurazione precedente aggiorna l'elenco dei pacchetti, scarica e installa gli aggiornamenti disponibili ogni giorno. L'archivio locale dei file scaricati viene pulito ogni settimana.

Maggiori informazioni sulle opzioni di configurazione della periodicità di apt possono essere trovate nell'intestazione dello script `/etc/cron.daily/apt`.

I risultati di unattended-upgrades vengono registrati in `/var/log/unattended-upgrades`.

5.1. Notifiche

Impostando *Unattended-Upgrade::Mail* nel file `/etc/apt/apt.conf.d/50unattended-upgrades`, si abilita unattended-upgrades all'invio di email all'amministratore indicando i pacchetti da aggiornare o con problemi.

Un altro pacchetto molto utile è apticron, che consente di configurare un lavoro cron per l'invio di email all'amministratore con informazioni sui pacchetti da aggiornare, oltre a un resoconto delle modifiche in ogni pacchetto.

Per installare apticron, digitare:

```
sudo apt-get install apticron
```

Una volta installato, aprire il file `/etc/apticron/apticron.conf` e impostare l'indirizzo email e altre opzioni:

```
EMAIL="root@example.com"
```

6. Configurazione

La configurazione dei repository del sistema *APT* (Advanced Packaging Tool) è memorizzata nel file `/etc/apt/sources.list` e nella directory `/etc/apt/sources.list.d`. Un esempio di questo file, con le istruzioni su come aggiungere e rimuovere repository, è qui referenziato.

È possibile modificare il file per abilitare o disabilitare i repository. Per esempio, per disabilitare la necessità di inserire il CD-ROM di Ubuntu ogni volta che viene effettuata un'operazione sui pacchetti, è sufficiente commentare la riga relativa al CD-ROM, che si trova all'inizio del file:

```
# no more prompting for CD-ROM please
# deb cdrom:[Ubuntu 12.10 _Quantal Quetzal_ - Release i386 (20111013.1)]/ quantal main restricted
```

6.1. Repository aggiuntivi

In aggiunta ai repository dei pacchetti disponibili per Ubuntu e supportati ufficialmente, esistono repository aggiuntivi mantenuti dalla comunità che aggiungono migliaia di pacchetti che possono essere installati. Due dei più popolari sono i repository *universe* e *multiverse*. Questi repository non sono ufficialmente supportati da Ubuntu ma, proprio perché sono mantenuti dalla comunità, di norma forniscono pacchetti che possono essere installati sul proprio computer senza rischi.

I pacchetti nel repository *multiverse* presentano spesso problemi di licenza che non gli permettono di essere distribuiti con un sistema operativo gratuito e potrebbero essere illegali in alcuni paesi.

Né il repository *universe* né quello *multiverse* contengono pacchetti supportati ufficialmente. In particolare, potrebbero non esserci aggiornamenti di sicurezza per tali pacchetti.

Sono disponibili molte altre sorgenti di pacchetti, alcune delle quali offrono solo un pacchetto, come nel caso di sorgenti di pacchetto fornite dallo sviluppatore di una singola applicazione. L'utilizzo di sorgenti di pacchetto non standard è rischioso, pertanto è necessario prestare la massima attenzione. È opportuno controllare la sorgente e i pacchetti in modo accurato prima di effettuare una qualsiasi installazione, poiché alcune sorgenti di pacchetto, e i rispettivi pacchetti, potrebbero rendere il sistema instabile e non funzionante sotto certi aspetti.

I repository *universe* e *multiverse*, in modo predefinito, sono abilitati, ma se si desidera disabilitarli è possibile modificare il file `/etc/apt/sources.list` e commentare le seguenti righe:

```
deb http://archive.ubuntu.com/ubuntu quantal universe multiverse
deb-src http://archive.ubuntu.com/ubuntu quantal universe multiverse

deb http://us.archive.ubuntu.com/ubuntu/ quantal universe
deb-src http://us.archive.ubuntu.com/ubuntu/ quantal universe
deb http://us.archive.ubuntu.com/ubuntu/ quantal-updates universe
deb-src http://us.archive.ubuntu.com/ubuntu/ quantal-updates universe
```

```
deb http://us.archive.ubuntu.com/ubuntu/ quantal multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ quantal multiverse
deb http://us.archive.ubuntu.com/ubuntu/ quantal-updates multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ quantal-updates multiverse

deb http://security.ubuntu.com/ubuntu quantal-security universe
deb-src http://security.ubuntu.com/ubuntu quantal-security universe
deb http://security.ubuntu.com/ubuntu quantal-security multiverse
deb-src http://security.ubuntu.com/ubuntu quantal-security multiverse
```

7. Riferimenti

La maggior parte di quanto discusso in questo capitolo è disponibile nella pagine man, molte delle quali sono reperibili anche in rete.

- La pagina della documentazione della comunità *InstallingSoftware*[2] contiene ulteriori informazioni.
- For more dpkg details see the *dpkg man page*[3].
- The *APT HOWTO*[4] and *apt-get man page*[5] contain useful information regarding apt-get usage.
- See the *aptitude man page*[6] for more aptitude options.
- La pagina *riguardo i repository*[7] della documentazione italiana, contiene maggiori informazioni su come aggiungere repository.

2 https://help.ubuntu.com/community/InstallingSoftware
3 http://manpages.ubuntu.com/manpages/quantal/en/man1/dpkg.1.html
4 http://www.debian.org/doc/manuals/apt-howto/
5 http://manpages.ubuntu.com/manpages/quantal/en/man8/apt-get.8.html
6 http://manpages.ubuntu.com/manpages/quantal/man8/aptitude.8.html
7 http://wiki.ubuntu-it.org/Repository

Capitolo 4. Rete

Le reti consistono in due o più dispositivi, come computer, stampanti e altri equipaggiamenti correlati, connessi tramite un cavo fisico oppure tramite collegamenti senza fili, con lo scopo di condividere e distribuire informazioni tra di loro.

Questa sezione fornisce informazioni generali e specifiche sulle reti (creare, modificare e gestire reti), compresa una panoramica sui concetti delle reti e discussioni dettagliate dei più comuni protocolli di rete.

1. Configurare la rete

Ubuntu è corredato da una serie di utilità grafiche per la configurazione dei dispositivi di rete. Questa sezione è diretta agli amministratori di server e si focalizza sulla gestione della rete da riga di comando.

1.1. Interfacce Ethernet

Le interfacce Ethernet sono identificate dal sistema con il nome convenzionale di *ethX*, dove la *X* rappresenta un valore numerico. La prima interfaccia Ethernet è tipicamente identificata come *eth0*, la seconda come *eth1*, e tutte le altre seguono in ordine numerico.

1.1.1. Identificare le interfacce Ethernet

Per identificare rapidamente tutte le interfacce Ethernet disponibili, è possibile usare il comando ifconfig, come indicato in seguito.

```
ifconfig -a | grep eth
eth0      Link encap:Ethernet  HWaddr 00:15:c5:4a:16:5a
```

Un'altra applicazione che può aiutare a identificare tutte le interfacce di rete disponibili nel sistema è il comando lshw. Nel seguente esempio, lshw mostra una singola interfaccia Ethernet con il nome logico di *eth0*, insieme a informazioni sul bus, dettagli sul driver e tutte le capacità supportate.

```
sudo lshw -class network
  *-network
       description: Ethernet interface
       product: BCM4401-B0 100Base-TX
       vendor: Broadcom Corporation
       physical id: 0
       bus info: pci@0000:03:00.0
       logical name: eth0
       version: 02
       serial: 00:15:c5:4a:16:5a
       size: 10MB/s
       capacity: 100MB/s
       width: 32 bits
       clock: 33MHz
       capabilities: (snipped for brevity)
       configuration: (snipped for brevity)
       resources: irq:17 memory:ef9fe000-ef9fffff
```

1.1.2. Nomi logici dell'interfaccia Ethernet

I nomi logici delle interfacce sono configurati nel file `/etc/udev/rules.d/70-persistent-net.rules.`. Per controllare quale interfaccia riceve un particolare nome logico, trovare la riga che corrisponde all'indirizzo MAC dell'interfaccia e modificare il valore *NAME=ethX* in quello desiderato. Riavviare il sistema per rendere definitive le modifiche.

1.1.3. Impostazione dell'interfaccia Ethernet

ethtool è un programma che visualizza e modifica impostazioni della scheda Ethernet come l'autonegoziazione, la velocità della porta, la modalità duplex e il Wake-on-LAN. Non è installato per impostazione predefinita, ma è disponibile per l'installazione da repository.

```
sudo apt-get install ethtool
```

Quello che segue è un esempio di come visualizzare caratteristiche supportate e impostazioni configurate di un'interfaccia Ethernet.

```
sudo ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: g
        Wake-on: d
        Current message level: 0x000000ff (255)
        Link detected: yes
```

Le modifiche effettuate mediante il comando ethtool sono temporanee e verranno perse dopo un riavvio. Per conservare le impostazioni, basta aggiungere l'appropriato comando ethtool a un'istruzione *pre-up* nel file di configurazione delle interfacce `/etc/network/interfaces`.

Ciò che segue è un esempio di come è possibile configurare permanentemente l'interfaccia identificata come *eth0* con una velocità di porta di 1000Mb/s in modalità full duplex.

```
auto eth0
iface eth0 inet static
pre-up /sbin/ethtool -s eth0 speed 1000 duplex full
```

Sebbene l'esempio mostri un'interfaccia configurata per utilizzare un metodo *statico*, funziona anche con altri metodi, come il DHCP. L'esempio vuole solo dimostrare la corretta posizione dell'istruzione *pre-up* in relazione alla rimanente parte della configurazione dell'interfaccia.

1.2. Indirizzamento IP

La seguente sezione descrive il processo di configurazione dell'indirizzo IP di sistema e del gateway predefinito necessari per le comunicazioni su una rete locale e Internet.

1.2.1. Assegnazione temporanea di un indirizzo IP

Per configurazioni di reti temporanee, è possibile utilizzare comandi standard come ip, ifconfig e route, che si trovano anche su molti altri sistemi operativi GNU/Linux. Questi comandi consentono di configurare impostazioni che hanno effetto immediatamente, ma non sono persistenti e verranno perse dopo un riavvio.

Per configurare temporaneamente un indirizzo IP, è possibile usare il comando ifconfig nella seguente maniera; basta modificare l'indirizzo IP e la maschera di sottorete per farli corrispondere ai requisiti della propria rete.

```
sudo ifconfig eth0 10.0.0.100 netmask 255.255.255.0
```

Per verificare la configurazione dell'indirizzo IP di eth0, è possibile usare il comando ifconfig nel seguente modo:

```
ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:15:c5:4a:16:5a
          inet addr:10.0.0.100  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::215:c5ff:fe4a:165a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:466475604 errors:0 dropped:0 overruns:0 frame:0
          TX packets:403172654 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2574778386 (2.5 GB)  TX bytes:1618367329 (1.6 GB)
          Interrupt:16
```

Per configurare un gateway predefinito, è possibile usare il comando route nel seguente modo; modificare l'indirizzo del gateway predefinito per farlo corrispondere ai requisiti della propria rete.

```
sudo route add default gw 10.0.0.1 eth0
```

Per verificare la configurazione del gateway predefinito, è possibile usare il comando route nel seguente modo:

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     1      0        0 eth0
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 eth0
```

Se per la configurazione della rete temporanea è necessario un DNS, è possibile aggiungere gli indirizzi IP del server DNS nel file `/etc/resolv.conf`. Il seguente esempio mostra come inserire

due server DNS in `/etc/resolv.conf`, da modificare nei server adeguati alla propria rete. Una più esaustiva descrizione della configurazione di un client DNS è contenuta nella sezione successiva.

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Se questa configurazione non è più necessaria ed è necessario eliminare tutte le configurazioni IP da un'interfaccia, è possibile usare il comando ip con l'opzione *flush*, come mostrato di seguito.

```
ip addr flush eth0
```

Usare il comando ip con l'opzione *flush* non ripulisce il contenuto di `/etc/resolv.conf`: è necessario rimuovere o modificare queste voci manualmente.

1.2.2. Assegnazione di un indirizzo IP dinamico (Client DHCP)

Per configurare il proprio server per usare DHCP per l'assegnazione di un indirizzo dinamico, aggiungere il metodo *dhcp* all'indirizzo inet nell'istruzione per l'interfaccia appropriata nel file `/etc/network/interfaces`. Il seguente esempio assume che si stia configurando la prima interfaccia Ethernet identificata come *eth0*.

```
auto eth0
iface eth0 inet dhcp
```

Nell'aggiungere una configurazione d'interfaccia come mostrato sopra, è possibile abilitare manualmente l'interfaccia con il comando ifup che inizializza il processo DHCP tramite dhclient.

```
sudo ifup eth0
```

Per disabilitare manualmente l'interfaccia, è possibile usare il comando ifdown, che avvia il processo di rilascio di DHCP e disattiva l'interfaccia.

```
sudo ifdown eth0
```

1.2.3. Assegnazione di un indirizzo IP statico

Per configurare il sistema per usare un'assegnazione di indirizzo IP statico, aggiungere il metodo *statico* all'indirizzo inet nell'istruzione per l'interfaccia appropriata nel file `/etc/network/interfaces`. Il seguente esempio assume che si stia configurando la prima interfaccia Ethernet identificata come *eth0*. Modificare i valori per l'*indirizzo*, la *maschera di rete* e il *gateway* per farli corrispondere ai requisiti della propria rete.

```
auto eth0
iface eth0 inet static
address 10.0.0.100
```

```
netmask 255.255.255.0
gateway 10.0.0.1
```

Nell'aggiungere una configurazione d'interfaccia come mostrato sopra, è possibile abilitare manualmente l'interfaccia con il comando ifup.

```
sudo ifup eth0
```

Per disabilitare manualmente l'interfaccia, è possibile usare il comando ifdown.

```
sudo ifdown eth0
```

1.2.4. Interfaccia di loopback

L'interfaccia di loopback è identificata dal sistema come *lo* e ha un indirizzo IP predefinito di 127.0.0.1; può essere visualizzata con il comando ifconfig.

```
ifconfig lo
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2718 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2718 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:183308 (183.3 KB)  TX bytes:183308 (183.3 KB)
```

Per impostazione predefinita, in `/etc/network/interfaces` sono presenti due righe responsabili della configurazione automatica dell'interfaccia di loopback. Si raccomanda di mantenere le impostazioni predefinite a meno che non ci sia una specifica necessità di modificarle. Di seguito viene mostrato un esempio delle due righe predefinite.

```
auto lo
iface lo inet loopback
```

1.3. Risoluzione del nome

La risoluzione del nome, in relazione alle reti IP, è il processo con cui vengono stabilite corrispondenze tra gli indirizzi IP e i nomi host, rendendo più semplice l'identificazione delle risorse su una rete. La seguente sezione spiega come configurare correttamente il proprio sistema per la risoluzione del nome usando record statici per i nomi host.

1.3.1. Configurazione del client DNS

Tradizionalmente, il file `/etc/resolv.conf` era un file di configurazione statico che raramente necessitava di essere modificato o di ricevere modifiche automatiche tramite indirizzatori client

DHCP. Al giorno d'oggi, un computer può spostarsi da una rete all'altra abbastanza frequentemente e l'infrastruttura *resolvconf* viene utilizzata per conservare traccia di queste modifiche e aggiornare automaticamente la configurazione del resolver. Agisce come intermediario fra i programmi che forniscono le informazioni sul server dei nomi e le applicazioni che necessitano di queste informazioni. Resolvconf viene popolato di informazioni da un insieme di script di indirizzamento collegati alla configurazione dell'interfaccia di rete. La più evidente differenza per l'utente consiste nel fatto che ogni modifica manuale effettuata in /etc/resolv.conf verrà persa e sovrascritta ogni volta che viene attivato resolvconf. Invece, resolvconf utilizza indirizzatori client DHCP e `/etc/network/interfaces` per generare un elenco di server dei nomi e di domini da collocare in /etc/resolv.conf, che è ora un collegamento simbolico:

```
/etc/resolv.conf -> ../run/resolvconf/resolv.conf
```

. Per configurare il resolver, aggiungere gli indirizzi IP dei server dei nomi appropriati per la propria rete nel file `/etc/network/interfaces`. È possibile anche aggiungere un elenco di ricerca di suffissi DNS opzionale per far corrispondere i nomi di dominio della propria rete. Per ciascuna ulteriore valida opzione di configurazione di resolv.conf, è possibile includere, nella sezione, una riga che inizia con il nome dell'opzione con un prefisso **dns-**. Il file risultante dovrebbe essere simile al seguente:

```
iface eth0 inet static
    address 192.168.3.3
    netmask 255.255.255.0
    gateway 192.168.3.1
    dns-search example.com
    dns-nameservers 192.168.3.45 192.168.8.10
```

L'opzione *search* può anche essere usata con nomi di domini multipli, così che le query DNS vengano accodate secondo l'ordine di immissione. Per esempio, la rete può avere un campo di ricerca in più sotto-domini; un dominio superiore *example.com* e due sotto-domini, *sales.example.com* e *dev.example.com*.

Se la ricerca deve essere effettuata in più domini, la configurazione dovrebbe essere simile alla seguente:

```
iface eth0 inet static
    address 192.168.3.3
    netmask 255.255.255.0
    gateway 192.168.3.1
    dns-search example.com sales.example.com dev.example.com
    dns-nameservers 192.168.3.45 192.168.8.10
```

Se si invia un ping a un host con nome *server1*, il sistema cercherà automaticamente in DNS il suo nome di dominio completo (Fully Qualified Domain Name - FQDN) nel seguente ordine:

1. server1**.example.com**

2. server1**.sales.example.com**
3. server1**.dev.example.com**

Se non vengono trovate corrispondenze, il server DNS fornisce un risultato di *notfound (non trovato)* e la query DNS fallirà.

1.3.2. Nomi host statici

I nomi host statici sono definiti localmente come corrispondenze tra nome host e IP, posizionati nel file `/etc/hosts`. Per impostazione predefinita, le voci nel file `hosts` hanno precedenza sul DNS. Ciò significa che se il sistema cerca di risolvere un nome host e trova una corrispondenza in /etc/hosts, non tenterà di cercare il record in DNS. In alcune configurazioni, specie quando non sia richiesto un accesso a Internet, i server che comunicano con un limitato numero di risorse possono essere opportunamente impostati per usare nomi host statici invece del DNS.

Ciò che segue è l'esempio di un file `hosts` dove alcuni server locali sono stati identificati con semplici nomi host, alias e i loro equivalenti nomi di dominio completi (Fully Qualified Domain Name - FQDN)

```
127.0.0.1 localhost
127.0.1.1 ubuntu-server
10.0.0.11 server1 vpn server1.example.com
10.0.0.12 server2 mail server2.example.com
10.0.0.13 server3 www server3.example.com
10.0.0.14 server4 file server4.example.com
```

Nel precedente esempio, notare come a ciascun server siano stati attribuiti degli alias, in aggiunta ai nomi propri e ai FQDN. *Server1* corrisponde al nome *vpn*, *server2* è riferito a *mail*, *server3* è *www* e *server4* è *file*.

1.3.3. Configurazione del Name Service Switch

L'ordine in cui il sistema seleziona un metodo per risolvere i nomi host in indirizzi IP è controllato dal file di configurazione del Name Service Switch (NSS) `/etc/nsswitch.conf`. Come illustrato nella precedente sezione, normalmente i nomi host statici definiti nel file di sistema `/etc/hosts` hanno precedenza sui nomi risolti dal DNS. Ciò che segue è un esempio della riga responsabile dell'ordine di ricerca dei nomi host in `/etc/nsswitch.conf`.

```
hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4
```

- Per prima cosa, **files** cerca di risolvere i nomi host statici che si trovano in `/etc/hosts`.
- **mdns4_minimal** tenta di risolvere il nome usando il DNS Multicast.
- **[NOTFOUND=return]** significa che ogni risposta *notfound* dal precedente processo *mdns4_minimal* viene considerata autoritativa e il sistema non tenterà di continuare a cercare una risposta.

- **dns** rappresenta una tradizionale query DNS Unicast.
- **mdns4** rappresenta una query DNS Multicast.

Per modificare l'ordine dei metodi di risoluzione dei nomi sopra menzionati, basta modificare la stringa *hosts:* nel valore prescelto. Per esempio, se si preferisce usare il tradizionale DNS Unicast invece del DNS Multicast, modificare la stringa in `/etc/nsswitch.conf` come indicato di seguito.

```
hosts: files dns [NOTFOUND=return] mdns4_minimal mdns4
```

1.4. Bridging

Il «bridging» di molteplici interfacce è una configurazione avanzata, ma utile in diversi scenari. Uno di questi scenari può consistere nel configurare un bridge con molteplici interfacce di rete e usare un firewall per filtrare il traffico tra due segmenti della rete. Un altro scenario consiste nell'usare un bridge su un sistema con una sola interfaccia per permettere alle macchine virtuali accesso diretto alla rete esterna. L'esempio che segue prende in considerazione quest'ultimo scenario.

Prima di configurare un bridge è necessario installare il pacchetto bridge-utils. In un terminale digitare:

```
sudo apt-get install bridge-utils
```

Configurare il bridge modificando il file `/etc/network/interfaces`:

```
auto lo
iface lo inet loopback

auto br0
iface br0 inet static
        address 192.168.0.10
        network 192.168.0.0
        netmask 255.255.255.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
        bridge_ports eth0
        bridge_fd 9
        bridge_hello 2
        bridge_maxage 12
        bridge_stp off
```

Inserire i valori appropriati per la propria interfaccia di rete.

Riavviare la rete per abilitare il bridge sull'interfaccia:

```
sudo service networking restart
```

La nuova interfaccia dovrebbe ora essere funzionante. L'applicazione brctl fornisce utili informazioni riguardo lo stato del bridge, controlla le interfacce che compongono il bridge, ecc... Per maggiori informazioni, consultare la pagina di manuale: **man brctl**.

1.5. Risorse

- La pagina della *documentazione della comunità sulle reti*[1] contiene link ad articoli che trattano la configurazione avanzata delle reti.
- Maggiori informazioni su resolvconf possono essere trovate sulla *relativa pagina del manuale*[2].
- La pagina del manuale *interfacce*[3] contiene ulteriori opzioni per `/etc/network/interfaces`.
- Dettagli su ulteriori opzioni per configurare client DHCP possono essere trovati nella *pagina del manuale dhclient*[4].
- Per ulteriori informazioni sulla configurazione di client DNS, consultare la pagina del manuale di *resolver*[5]. Anche il Capitolo 6 della *Linux Network Administrator's Guide*[6] di O'Reilly è una buona fonte di informazioni sulla configurazione di resolver e name service.
- Per maggiori informazioni sul *bridging*, consultare la *pagina del manuale di brctl*[7] e la pagina *Net:Bridge*[8] della Linux Foundation.

[1] https://help.ubuntu.com/community/Network
[2] http://manpages.ubuntu.com/manpages/man8/resolvconf.8.html
[3] http://manpages.ubuntu.com/manpages/man5/interfaces.5.html
[4] http://manpages.ubuntu.com/manpages/man8/dhclient.8.html
[5] http://manpages.ubuntu.com/manpages/man5/resolver.5.html
[6] http://oreilly.com/catalog/linag2/book/ch06.html
[7] http://manpages.ubuntu.com/manpages/man8/brctl.8.html
[8] http://www.linuxfoundation.org/en/Net:Bridge

2. TCP/IP

Il protocollo TCP/IP (Transmission Control Protocol e Internet Protocol) è un insieme standard di protocolli sviluppato nella seconda metà degli anni '70 dalla DARPA (Defence Advanced Research Project Agency) con lo scopo di permettere la comunicazione tra diversi tipi di computer e di reti di computer. TCP/IP è il motore di Internet, ecco perché è l'insieme di protocolli di rete più diffuso al mondo.

2.1. Introduzione a TCP/IP

I due protocolli che compongono TCP/IP, interagiscono con differenti aspetti di una rete. L'*Internet Protocol*, la parte «IP» di TCP/IP, è un protocollo privo di connessione che interagisce solamente con il routing dei pacchetti attraverso la rete, usando l'*IP Datagram* come unità di base delle informazioni che consiste in un'intestazione seguita da un messaggio. Il *Transmission Control Protocol*, la parte «TCP» di TCP/IP, consente agli host della rete di stabilire le connessioni che possono essere usate per scambiare dati. Inoltre, garantisce che i dati tra le connessioni siano consegnati correttamente e nello stesso ordine in cui sono stati inviati.

2.2. Configurazione di TCP/IP

La configurazione del protocollo TCP/IP è composta da vari elementi che debbono essere impostati modificando gli appropriati file di configurazione oppure adottando soluzioni quali un server DHCP (Dynamic Host Configuration Protocol); tale server provvede ad assegnare automaticamente le corrette impostazioni di configurazione TCP/IP ai client della rete. Questi valori di configurazione debbono essere impostati correttamente per consentire al sistema Ubuntu di operare adeguatamente in rete.

I tipici elementi di configurazione di TCP/IP e i loro scopi sono i seguenti:

- **Indirizzo IP**: l'indirizzo IP è una stringa d'identificazione unica, espressa da quattro numeri decimali compresi tra zero (0) e duecentocinquantacinque (255), separati da punti; ciascuno dei quattro numeri rappresenta otto (8) bit dell'indirizzo per una lunghezza totale di trentadue (32) bit per l'indirizzo completo. Questo formato è detto *notazione decimale a punti*.
- **Maschera di rete**: la maschera di rete (o semplicemente *netmask*) è una maschera locale di bit, ovvero un insieme di indicatori che separano la porzione di un indirizzo IP che indica la rete dai bit che indicano la *sotto-rete*. Ad esempio, in una rete di classe C, la maschera di rete standard è 255.255.255.0 che serve a mascherare i primi tre byte dell'indirizzo IP, consentendo all'ultimo byte dell'indirizzo IP di essere disponibile per specificare gli host della sotto-rete.
- **Indirizzo di rete**: l'indirizzo di rete è dato dai byte che comprendono la parte di rete di un indirizzo IP. Per esempio, l'host 12.128.1.2 in una rete di classe A deve usare 12.0.0.0 come indirizzo di rete, dove dodici (12) è il primo byte dell'indirizzo IP (la parte di rete), e gli zeri (0) nei rimanenti tre byte indicano tutti i possibili valori degli host. Un host di rete che ha un indirizzo IP 192.168.1.100 deve invece usare un indirizzo di rete di 192.168.1.0, nel quale i primi tre byte specificano la rete di classe C 192.168.2 e lo zero (0) per tutti i possibili valori degli host nella rete.

- **Indirizzo di broadcast**: l'indirizzo di broadcast è un indirizzo IP che permette di inviare dei dati di rete simultaneamente a tutti gli host di una data sotto-rete piuttosto che a uno specifico host. L'indirizzo broadcast generale di base per una rete IP è 255.255.255.255, ma questo indirizzo broadcast non può essere usato per inviare un messaggio broadcast a tutti gli host presenti in internet perché i router lo bloccherebbero. Un indirizzo di broadcast appropriato è quello che indica una specifica sotto-rete. Per esempio, in una rete privata di classe C, 192.168.1.0, l'indirizzo broadcast è 192.168.1.255. I messaggi broadcast sono di norma prodotti dai protocolli di rete come il protocollo per la risoluzione degli indirizzi (ARP, Address Resolution Protocol) e il protocollo delle informazioni di instradamento (RIP, Routing Information Protocol).
- **Indirizzo del gateway**: l'indirizzo del gateway è l'indirizzo IP attraverso il quale una particolare rete, o un host su una rete, può essere raggiunta. Se un host di rete desidera comunicare con un altro host di rete, senza essere localizzato nelle stessa rete, allora deve essere usato un *gateway*. In molti casi l'indirizzo del gateway coincide con quello di un router della medesima rete che ha il compito di far transitare il traffico ad altre reti o host, come Internet. L'impostazione del valore dell'indirizzo del gateway deve essere corretta, altrimenti il sistema non è in grado di raggiungere gli host che non si trovano sulla rete cui appartiene.
- **Indirizzo del server dei nomi**: l'indirizzo del server dei nomi rappresenta l'indirizzo IP del sistema DNS (Domain Name Service) che traduce il nome host della rete in un indirizzo IP reale. Esistono tre livelli di indirizzo del server dei nomi che possono essere specificati in ordine di precedenza: il server dei nomi *primario*, quello *secondario* e il *terziario*. Affinché il sistema possa tradurre i nomi host in indirizzi IP, è necessario specificare degli indirizzi validi per i server dei nomi che è possibile utilizzare all'interno della configurazione TCP/IP del sistema. Nella maggior parte dei casi, questi indirizzi vengono forniti dal proprio fornitore di servizio Internet, ma ne sono disponibili anche di gratuiti e liberamente utilizzabili, come i server di terzo livello di Verizon con indirizzi IP da 4.2.2.1 a 4.2.2.6.

Gli indirizzi IP, le maschere di rete, gli indirizzi di rete, gli indirizzi di broadcast e gli indirizzi di gateway sono tipicamente determinati attraverso appropriate direttive nel file `/etc/network/interfaces`. Gli indirizzi di server dei nomi sono tipicamente specificati attraverso le direttive *nameserver* nel file `/etc/resolv.conf`. Per maggiori informazioni, consultare rispettivamente le pagine di manuale di sistema per `interfaces` e `resolv.conf`, usando i seguenti comandi da digitare al prompt di un terminale:

Accedere alla pagina di manuale di sistema per `interfaces` con il seguente comando:

```
man interfaces
```

Accedere alla pagina di manuale di sistema per `resolv.conf` con il seguente comando:

```
man resolv.conf
```

2.3. Instradamento IP

L'instradamento IP è un modo per indicare e scoprire percorsi in una rete TCP/IP attraverso i quali inviare dati. L'instradamento utilizza un insieme di *tabelle di instradamento (routing)* per dirigere i pacchetti di dati in una rete dalla loro sorgente avanti fino alla destinazione, spesso attraverso molti nodi di rete intermediari chiamati *router*. Esistono due forme primarie di instradamento IP: l'*instradamento statico* e l'*instradamento dinamico*.

L'instradamento statico comporta l'aggiunta manuale di rotte IP nella tabella di instradamento del sistema, attività che viene fatta modificando la tabella di instradamento con il comando route. L'instradamento statico presenta molti vantaggi rispetto quello dinamico, come la semplicità di implementazione per piccole reti, la predicibilità (la tabella di instradamento è scritta a priori, quindi la rotta è sempre la stessa ogni volta che viene utilizzata) e il basso carico di lavoro sugli altri router e nodi di rete dovuto all'assenza di un protocollo di instradamento dinamico. In ogni caso, l'instradamento statico presenta anche degli svantaggi. Per esempio, è limitato a piccole reti e non è facilmente espandibile. L'instradamento statico fallisce completamente se si prova ad adattarlo ai ritardi della rete e le perdite lungo la rotta per la natura statica della rotta stessa.

L'instradamento dinamico serve nelle grandi reti con molte possibili rotte IP tra una sorgente e una destinazione. Fa uso di protocolli di instradamento speciali, come il protocollo di informazione dell'instradamento (RIP, Router Information Protocol) che gestisce le correzioni automatiche nella tabella di instradamento rendendo possibile l'instradamento dinamico. Ci sono molti vantaggi rispetto l'instradamento statico, come l'adattamento alle dimensioni superiori e l'abilità di adattarsi agli errori e alle perdite lungo le rotte della rete. Inoltre, necessita di una minore configurazione manuale delle tabelle di instradamento, dato che i router comunicano tra di loro la relativa esistenza e le possibili rotte. Questo tratto caratteristico elimina anche la possibilità di introdurre inesattezze nelle tabelle di instradamento causate da errori umani. In ogni caso, l'instradamento dinamico non è perfetto e presenta alcuni svantaggi come, l'aumento della complessità e del carico di lavoro dovuto alle comunicazioni dei router della rete, dei quali non può beneficiare subito l'utente finale che comunque consuma banda di rete.

2.4. TCP e UDP

TCP è un protocollo basato sulla connessione, che offre correzione d'errore e che garantisce la consegna dei dati attraverso ciò che è conosciuto come *controllo di flusso*. Il controllo di flusso determina quando il flusso di uno stream di dati debba essere fermato e i pacchetti di dati inviati in precedenza debbano essere reinviati a causa di problemi come *collisioni*, assicurando quindi la completa e accurata consegna dei dati. TCP è tipicamente usato nello scambio di informazioni importanti come transazioni di database.

UDP (User Datagram Protocol), al contrario, è un protocollo *senza connessione* che raramente tratta della trasmissione dei dati importanti a causa della mancanza del controllo di flusso o di un altro metodo che garantisca la consegna affidabile dei dati. UDP è normalmente usato in applicazioni come lo streaming audio e video, in cui risulta considerevolmente più veloce del protocollo TCP, data la

mancanza di correzione d'errore e del controllo di flusso, e in cui la perdita di alcuni pacchetti non è generalmente un evento catastrofico.

2.5. ICPM

ICMP (Internet Control Messaging Protocol) è un'estensione di IP (Internet Protocol), come definito nell'RFC (Request For Comments) numero 792; ICPM supporta pacchetti di rete contenenti messaggi di controllo, di errore e di informazione. ICMP è usato da applicazioni di rete come l'utilità ping, che consente di determinare la disponibilità di un host o un'interfaccia di rete. Esempi di alcuni dei messaggi di errore restituiti da ICMP utili sia agli host e interfacce di rete che ai router sono *Destination Unreachable* e *Time Exceeded*.

2.6. Demoni

I demoni sono speciali applicazioni di sistema che, tipicamente, sono in continua esecuzione sullo sfondo, attendendo dagli altri programmi richieste relative a funzioni da essi fornite. Molti demoni hanno a che fare con la rete e molti di questi in esecuzione sullo sfondo nei sistemi Ubuntu forniscono delle funzionalità legate alla rete. Alcuni esempi di questi demoni di rete includono *httpd* (Hyper Text Transport Protocol Daemon), che fornisce funzionalità di server web; *sshd* (Secure SHell Daemon), che fornisce funzionalità di login e trasferimento file sicuro da remoto; *imapd* (Internet Message Access Protocol Daemon), che fornisce servizi di email.

2.7. Risorse

- There are man pages for *TCP*[9] and *IP*[10] that contain more useful information.
- Inoltre, consultare il RedBook di IBM: *TCP/IP Tutorial and Technical Overview*[11].
- Un'altra utile risorsa è il libro *TCP/IP Network Administration*[12].

[9] http://manpages.ubuntu.com/manpages/quantal/en/man7/tcp.7.html
[10] http://manpages.ubuntu.com/manpages/quantal/man7/ip.7.html
[11] http://www.redbooks.ibm.com/abstracts/gg243376.html
[12] http://oreilly.com/catalog/9780596002978/

3. DHCP (Dynamic Host Configuration Protocol)

Il DHCP (Dynamic Host Configuration Protocol) è un servizio di rete che consente di assegnare automaticamente le impostazioni per agli host da un server, senza la necessità di dover configurare manualmente ogni singolo host nella rete. I computer configurati per essere client DHCP non hanno alcun controllo sulle impostazioni che ricevono dal server DHCP e la configurazione è trasparente all'utente del computer.

Le impostazioni comuni fornite da un server DHCP a un client includono:

- Indirizzo IP e maschera di rete
- Indirizzo IP del gateway predefinito da utilizzare
- Indirizzo IP del server DNS da utilizzare

Un server DHCP può fornire anche altre proprietà di configurazione come:

- Nome dell'host
- Nome del dominio
- Server NTP (Network Time Protocol)
- Server di stampa

Il vantaggio di utilizzare DHCP è che i cambiamenti apportati alla rete, per esempio una modifica dell'indirizzo del server DNS, devono essere apportati solamente al server DHCP, mentre tutti gli host della rete vengono riconfigurati quando i client DHCP interrogano il server DHCP. Come ulteriore vantaggio, risulta anche molto semplice integrare nuovi computer nella rete, senza la necessità di controllare la disponibilità di un indirizzo IP. I conflitti nell'allocazione degli indirizzi IP sono quindi notevolmente ridotti.

Un server DHCP può fornire impostazioni di configurazione usando i seguenti metodi:

Allocazione manuale (indirizzo MAC)

Questo metodo comporta l'utilizzo di DHCP per identificare l'indirizzo hardware univoco di ogni scheda di rete collegata alla rete, così da fornire in modo continuato una configurazione costante ogni volta che il client DHCP avanza una richiesta al server DHCP usando quel particolare dispositivo di rete. Ciò assicura che un particolare indirizzo sia assegnato automaticamente a una data scheda di rete, in base all'indirizzo MAC.

Allocazione dinamica (spazio di indirizzi)

In questo metodo, il server DHCP assegna un indirizzo IP preso da uno spazio di indirizzi (talvolta chiamato anche intervallo o insieme) per un periodo di tempo (detto «affitto») configurato sul server o fino a quando il client comunica al server che l'indirizzo richiesto non è più necessario. In questo modo i client ricevono le proprietà di configurazione in maniera dinamica, in base all'ordine di arrivo delle richieste. Dopo un determinato periodo, se il client DHCP non è più presente in rete, la configurazione scade e viene reinserita nello spazio di indirizzi per poter essere riutilizzata da altri client DHCP. In questo modo, un indirizzo può essere «affittato» o usato per un periodo di tempo, trascorso il quale, il client deve rinegoziare «l'affitto» con il server per conservare il diritto di usare l'indirizzo.

Allocazione automatica

Usando questo metodo, il DHCP assegna automaticamente indirizzi IP permanentemente a un dispositivo, selezionandoli da un insieme di indirizzi disponibili. Di solito DHCP è usato per assegnare un indirizzo temporaneo al client, ma un server DHCP può consentire un tempo di utilizzo infinito.

Gli ultimi due metodi possono essere definiti «automatici» in quanto in ciascun caso il server DHCP assegna un indirizzo senza necessità di un intervento aggiuntivo. L'unica differenza tra di essi è data dalla lunghezza del periodo di «affitto», in altri termini dalla variazione dell'indirizzo del client nel tempo. Ubuntu comprende sia un server che un client DHCP. Il server è dhcpd (dynamic host configuration protocol daemon); il client fornito è dhclient e dovrebbe essere installato su tutti i computer che necessitano di essere configurati automaticamente. Entrambi i programmi sono facili da installare e da configurare e vengono lanciati automaticamente all'avvio del sistema.

3.1. Installazione

A un prompt di terminale, inserire il seguente comando per installare dhcpd:

```
sudo apt-get install isc-dhcp-server
```

È necessario modificare il file predefinito /etc/dhcp/dhcpd.conf per adattarlo alle proprie necessità e per avere una configurazione particolare.

È inoltre necessario modificare il file /etc/default/isc-dhcp-server per specificare le interfacce su cui rimanere in ascolto.

I messaggi di dhcpd vengono inviati nel syslog, consultare quindi i relativi messaggi per quelli di diagnostica.

3.2. Configurazione

Il messaggio di errore con cui si conclude l'installazione potrebbe essere fuorviante, ma i passi seguenti consentono di configurare il servizio.

Nella maggior parte dei casi si vuole assegnare un indirizzo IP in modo casuale. Questo può essere ottenuto con impostazioni come le seguenti:

```
# minimal sample /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.150 192.168.1.200;
 option routers 192.168.1.254;
 option domain-name-servers 192.168.1.1, 192.168.1.2;
 option domain-name "mydomain.example";
```

```
}
```

Come risultato si ottiene che il server DHCP fornisce ai client un indirizzo IP nell'intervallo 192.168.1.150 - 192.168.1.200. Se il client non richiede uno specifico intervallo di tempo, la durata di «affitto» di un indirizzo IP è di 600 secondi; in caso contrario il valore massimo (consentito) è di 7200 secondi. Il server inoltre «consiglia» al client l'utilizzo di 192.168.1.254 come gateway predefinito, 192.168.1.1 e 192.168.1.2 come server DNS.

Dopo aver modificato il file di configurazione, è necessario riavviare dhcpd:

```
sudo service isc-dhcp-server restart
```

3.3. Riferimenti

- Per maggiori informazioni, consultare la pagina della *documentazione della comunità su dhcp3-server*[13].
- For more `/etc/dhcp/dhcpd.conf` options see the *dhcpd.conf man page*[14].
- *ISC dhcp-server*[15]

[13] https://help.ubuntu.com/community/dhcp3-server
[14] http://manpages.ubuntu.com/manpages/quantal/en/man5/dhcpd.conf.5.html
[15] http://www.isc.org/software/dhcp

4. Sincronizzazione del tempo con NTP

NTP è un protocollo TCP/IP per sincronizzare l'ora attraverso la rete: un client richiede l'ora corrente a un server e usa questa per impostare il proprio orologio.

Dietro questa semplice descrizione c'è molta complessità - ci sono vari livelli di server NTP, con il primo livello di server NTP collegati a orologi atomici e il secondo e terzo livello di server che si dividono il carico di gestire le richieste che pervengono da Internet. Anche il programma client è molto più complesso di quanto si possa pensare: deve considerare i ritardi di comunicazione e correggere l'ora in modo tale da non invalidare tutti gli altri processi che sono in esecuzione sul server. Fortunatamente tutta questa complessità è nascosta all'utente.

Ubuntu usa ntpdate and ntpd.

4.1. ntpdate

Ubuntu dispone di ntpdate come programma standard che viene eseguito all'avvio per impostare l'ora in base al server NTP di Ubuntu.

```
ntpdate -s ntp.ubuntu.com
```

4.2. ntpd

Ntpd, il demone di ntp, calcola lo spostamento dell'orologio del proprio sistema e lo regola continuamente, così non ci siano mai grandi modifiche che possono portare a file di registro inconsistenti. Il costo di questo è un leggero uso di processore e memoria, trascurabile per un server moderno.

4.3. Installazione

Per installare ntpd, digitare in un terminale:

```
sudo apt-get install ntp
```

4.4. Configurazione

Modificare `/etc/ntp.conf` per aggiungere/rimuovere linee di server: per impostazione predefinita questi server sono configurati:

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
```

```
server 3.ubuntu.pool.ntp.org
```

Dopo aver modificato il file di configurazione è necessario ricaricare ntpd:

```
sudo service ntp reload
```

4.5. Visualizzare lo stato

Usare ntpq per visualizzare maggiori informazioni:

```
# sudo ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+stratum2-2.NTP. 129.70.130.70    2 u    5   64  377   68.461  -44.274 110.334
+ntp2.m-online.n 212.18.1.106     2 u    5   64  377   54.629  -27.318  78.882
*145.253.66.170  .DCFa.           1 u   10   64  377   83.607  -30.159  68.343
+stratum2-3.NTP. 129.70.130.70    2 u    5   64  357   68.795  -68.168 104.612
+europium.canoni 193.79.237.14    2 u   63   64  337   81.534  -67.968  92.792
```

4.6. Riferimenti

- Per maggiori informazioni, consultare la documentazione della comunità *Ubuntu Time*[16].
- *ntp.org, sito web del progetto Network Time Protocol*[17]

[16] https://help.ubuntu.com/community/UbuntuTime
[17] http://www.ntp.org/

Capitolo 5. DM-Multipath

1. Device Mapper Multipathing

§Il Device mapper multipathing (DM-Multipath) permette di configurare percorsi I/O multipli tra i nodi del server e gli array di archiviazione in un dispositivo singolo. I suddetti percorsi I/O sono collegamenti SAN fisici che possono includere cavi, interruttori e controller separati. Multipathing aggrega i percorsi I/O, creando un nuovo dispositivo che consisterà di percorsi aggregati. Questo capitolo fornisce un sommario delle nuove caratteristiche di DM-Multipath per la release iniziale di Ubuntu Server 12.04. A seguire verrà fornita una panoramica dettagliata di DM Multipath e dei suoi componenti insieme ad una panoramica sulla sua impostazione.

1.1. Funzioni nuove e modificate per Ubuntu Server 12.04

Magrate da multipath-0.4.8 a multipath-0.4.9

1.1.1. Migrazione da 0.4.8

I controllori di priorità non sono più eseguiti come codici binari autonomi ma come librerie condivise; anche il nome del valore chiave per questa caratteristica è stato leggermente modificato. Copiare l'attributo chiamato **prio_callout** in **prio**, modificare anche l'argomento del nome del controllore di priorità, un percorso di sistema non più necessario. Esempio di conversione:

```
device {
         vendor "NEC"
         product "DISK ARRAY"
         prio_callout mpath_prio_alua /dev/%n
         prio alua
 }
```

See Table *Conversione del controllore di priorità [54]* for a complete listing

Tabella 5.1. Conversione del controllore di priorità

v0.4.8	v0.4.9
prio_callout mpath_prio_emc /dev/%n	**prio emc**
prio_callout mpath_prio_alua /dev/%n	**prio alua**
prio_callout mpath_prio_netapp /dev/%n	**prio netapp**
prio_callout mpath_prio_rdac /dev/%n	**prio rdac**
prio_callout mpath_prio_hp_sw /dev/%n	**prio hp_sw**
prio_callout mpath_prio_hds_modular %b	**prio hds**

Dal momento che il decodificatore del file di configurazione di multipath essenzialmente analizza tutte le coppie chiave/valore che trova per poi utilizzarle, è ragionevole che sia **prio_callout** che **prio** coesistano e si consiglia di inserire l'attributo **prio** prima di iniziare la migrazione. Dopo di ciò è possibile eliminare in sicurezza **prio_calliout**.

1.2. Panoramica

Il DM-Multipath può essere utilizzato per fornire:

- *Ridondanza* DM-Multipath permette il verificarsi di un failover in una configurazione attiva/passiva, nella quale solo metà dei percorsi vengono usati in qualsiasi momento per l'I/O. Se un elemento di un percorso di I/O (il cavo, l'interruttore o il controller) viene interrotto, DM-Multipath si sposta su di un percorso alternativo.
- *Migliori prestazioni* La prestazione di DM-Multipath può essere configurata in modalità attiva/attiva, in cui l'I/O viene suddiviso tra i percorsi seguendo un ordine round-robin. In alcune configurazioni, DM-Multipath è in grado di rilevare e bilanciare dinamicamente il carico sui percorsi di I/O.

1.3. Panoramica sull'array di archiviazione

Per impostazione predefinita, DM-Multipath include il supporto per gli array di archiviazione più comuni che supportano DM-Multipath. I dispositivi supportati sono disponibili nel file multipath.conf.defaults. Se l'array di archiviazione supporta DM-Multipath e non è configurato per impostazione predefinita, è necessario aggiungerlo al file di configurazione di DM-Multipath, multipath.conf. Per informazioni sul file di configurazione di DM-Multipath, consultare la *relativa Sezione*. Alcuni array di archiviazione richiedono una gestione speciale degli errori di I/O e dello smistamento del percorso. Questi processi necessitano di moduli del kernel gestore hardware separati.

1.4. Componenti DM-Multipath

La tabella *Componenti DM-Multipath* descrive i componenti del pacchetto DM-Multipath.

1.5. Panoramica sull'impostazione di DM-Multipath

DM-Multipath comprende impostazioni predefinite già compilate che sono adatte a configurazioni comuni di multipath; l'impostazione di DM-Multipath è spesso semplice; la procedura di base per configurare il sistema con DM-Multipath è la seguente:

1. Installare i pacchetti **multipath-tools** e **multipath-tools-boot**
2. Creare un file di configurazione vuoto, `/etc/multipath.conf`, che ridefinisce il *seguente*
3. Se necessario, modificare il file di configurazione **multipath.conf** per cambiare i valori predefiniti e salvare il file aggiornato.
4. Avviare il demone di multipath.
5. Aggiornare il ramdisk iniziale

. Per dettagliare istruzioni sull'impostazione della configurazione di multipath, consultare la Sezione *Impostazione di DM-Multipath*.

2. Dispositivi multipath

Senza DM-Multipath, ogni percorso proveniente da un nodo del server per un controller di archiviazione verrà considerato dal sistema come un dispositivo separato, anche quando il percorso di I/O collega lo stesso nodo del server al medesimo controller. DM-Multipath fornisce un modo con il quale è possibile organizzare logicamente i percorsi di I/O, attraverso la creazione di un dispositivo multipath singolo al di sopra dei dispositivi interessati.

2.1. Identificatori del dispositivo multipath

Ogni dispositivo multipath possiede un World Wide Identifier (WWID) unico ed immutabile; per impostazione predefinita il nome di un dispositivo multipath viene impostato seguendo il proprio WWID. In alternativa è possibile l'opzione ***user_friendly_names*** nel file di configurazione di multipath, che imposta l'alias su di un nome unico del nodo con il formato **mpathn**. Per esempio, un nodo con due HBA collegato tramite un interruttore FC singolo a un controller di archiviazione con due porte, è in grado di visualizzare quattro dispositivi: **/dev/sda**, **/dev/sdb**, **/dev/sdc** e **/dev/sdd**. DM-Multipath crea un dispositivo singolo con un unico WWID che instrada l'I/O ai sottostanti quattro dispositivi in base alla configurazione di multipath. Quando l'opzione di configurazione ***user_friendly_names*** è impostata su **yes**, il nome del dispositivo multipath viene impostato su **mpathn**. Quando DM-Multipath controlla nuovi dispositivi, essi potrebbero essere visti in due luoghi diversi sotto le directory **/dev/mapper/mpathn** e **/dev/dm-n**.

- I dispositivi in **/dev/mapper** sono creati precocemente durante il processo di avvio; possono essere usati per accedere ai dispositivi sui quali è stato eseguito multipath, per esempio durante la creazione dei volumi logici.
- Ogni dispositivo nel formato **/dev/dm-n** sarà per un uso solo interno e non deve essere mai usato.

Per informazioni sulla configurazione predefinita di multipath, compresa l'opzione di configurazione ***user_friendly_names***, consultare la Sezione *Impostazioni predefinite del file di configurazione*. È anche possibile scegliere un diverso nome per un dispositivo utilizzando l'opzione ***alias*** nella sezione **multipaths** del file di configurazione di multipath. Per informazioni su tale sezione, consultare *Attributi per la configurazione del dispositivo multipath*.

2.2. Nomi coerenti del dispositivo multipath in un cluster

Quando l'opzione di configurazione **user_friendly_names** è impostata su «yes», il nome del dispositivo multipath risulta essere unico per il nodo, ma non è garantito che sia lo stesso su tutti i nodi che usano il dispositivo multipath. Allo stesso modo, se viene impostata l'opzione **alias** per un dispositivo nella sezione **multipaths** del file di configurazione `multipath.conf`, il nome non sarà automaticamente coerente attraverso tutti i nodi del cluster. Ciò non dovrebbe causare alcun problema se si utilizza LVM durante la creazione dei dispositivi logici dal dispositivo multipath, ma se è necessario avere nomi uniformi del dispositivo multipath in ogni nodo del cluster, occorre lasciare l'opzione **user_friendly_names** impostata su **«no»** e non configurare alias per i dispositivi. Per impostazione predefinita, se non si imposta **user_friendly_names** su «yes» o non si configura un

alias per il dispositivo, il nome del dispositivo sarà il suo WWID, che sarà sempre lo stesso. Tuttavia, se è necessario che i nomi descrittivi assegnati dal sistema siano coerenti attraverso tutti i nodi nel cluster, occorre seguire la seguente procedura:

1. Impostare tutti i dispositivi multipath su una sola macchina.
2. Disabilitare tutti i dispositivi multipath sulle altre macchine, eseguendo i seguenti comandi:

```
# service multipath-tools stop
# multipath -F
```

3. Copiare il file `/etc/multipath/bindings` dalla prima macchina in tutte le altre macchine del cluster.
4. Abilitare nuovamente il demone multipathd su tutte le altre macchine del cluster con il seguente comando:

```
# service multipath-tools start
```

Se viene aggiunto un nuovo dispositivo, è necessario ripetere questo processo.

Analogamente, se è necessario che un alias configurato per un dispositivo sia coerente attraverso i nodi del cluster, occorre assicurarsi che il file `/etc/multipath.conf` sia lo stesso per ogni nodo del cluster seguendo la stessa procedura:

1. Configurare gli alias per i dispositivi multipath nel file `multipath.conf` su una macchina.
2. Disabilitare tutti i dispositivi multipath sulle altre macchine, eseguendo i seguenti comandi:

```
# service multipath-tools stop
# multipath -F
```

3. Copiare il file `multipath.conf` dalla prima macchina in tutte le altre macchine del cluster.
4. Abilitare nuovamente il demone multipathd su tutte le altre macchine del cluster con il seguente comando:

```
# service multipath-tools start
```

Quando viene aggiunto un nuovo dispositivo, è necessario ripetere questo processo.

2.3. Attributi del dispositivo multipath

Oltre alle opzioni **user_friendly_names** e **alias**, un dispositivo multipath ha numerosi attributi. È possibile modificare questi attributi per uno specifico dispositivo multipath creando una voce per quel dispositivo nella sezione **multipaths** del file di configurazione di **multipath**. Ulteriori informazioni su questa sezione possono essere ottenute consultando la sezione «*Attributi del file di configurazione di multipath*"».

2.4. Dispositivi multipath nei volumi logici

Dopo la creazione dei dispositivi multipath è possibile utilizzare i nomi del dispositivo multipath in modo simile al nome del dispositivo fisico usato durante la creazione di un volume fisico di LVM.

Per esempio, se /dev/mapper/mpatha è il nome di un dispositivo multipath, il seguente comando contrassegna /dev/mapper/mpatha come un volume fisico.

```
# pvcreate /dev/mapper/mpatha
```

Durante la creazione di un gruppo di volumi LVM è possibile utilizzare il dispositivo fisico LVM risultante in modo simile all'utilizzo di qualsiasi altro dispositivo fisico LVM.

Se si tenta di creare un volume fisico LVM su di un intero dispositivo sul quale sono state configurate delle partizioni, il comando pvcreate fallirà.

Quando viene creato un volume logico LVM che utilizza degli array multipath attivi/passivi come dispositivi fisici sottostanti, è necessario includere i filtri all'interno di **lvm.conf** in modo da escludere i dischi che costituiscono i dispositivi multipath. Questo comportamento si verifica poichè se l'array modifica automaticamente il percorso attivo in passivo una volta ricevuto un segnale di I/O, multipath eseguirà un failover e un failback ogni qualvolta LVM esegue una scansione del percorso passivo, se questi dispositivi non sono filtrati. Per array attivi/passivi che richiedono un comando per modificare un percorso da passivo ad attivo, LVM stampa un messaggio di avvertimento al verificarsi di tale evento. Per filtrare tutti i dispositivi SCSI nel file di configurazione LVM (lvm.conf), includere il seguente filtro nella sezione dispositivi del file.

```
filter = [ "r/block/", "r/disk/", "r/sd.*/", "a/.*/" ]
```

Dopo aver aggiornato `/etc/lvm.conf`, è necessario aggiornare l'**initrd**, in modo che questo file sia copiato nella posizione in cui il filtro è maggiormente necessario, durante l'avvio. Eseguire:

```
update-initramfs -u -k all
```

Ogni volta che vengono aggiornati sia `/etc/lvm.conf` che `/etc/multipath.conf`, è necessario ricostruire initrd in modo da rispecchiare queste modifiche. Ciò è indispensabile nel caso in cui siano necessari blacklist o filtri per mantenere una configurazione di archiviazione stabile.

3. Panoramica sull'impostazione di DM-Multipath

Questa sezione contiene esempi passo-passo di procedure per la configurazione di DM-Multipath. Al suo interno sono contenute le seguenti procedure:

- Impostazione di base di DM-Multipath
- Ignorare i dischi locali
- Aggiungere ulteriori dispositivi al file di configurazione

3.1. Impostare DM-Multipath

Prima di impostare DM-Multipath sul sistema, assicuratevi che il sistema stesso sia stato aggiornato e includa il pacchetto **multipath-tools**. Se è necessario effettuare l'avvio da una SAN, occorre anche il pacchetto **multipath-tools-boot**.

Una necessità di base di **/etc/multipath.conf** non esiste nemmeno, quando **multpath** è eseguito senza l'abbinamento con un `/etc/multipath.conf`, ricava un'adeguata configurazione dal suo database interno, e attinge anche dalla sua blacklist interna. Se dopo aver eseguito **multipath -ll** senza un file di configurazione non vengono scoperti multipath, è necessario procedere a un aumento della prolissità per scoprire perché non è stato creato un multipath. Fare riferimento alla documentazione del fornitore della SAN, ai file di configurazione di multipath forniti come esempio in `/usr/share/doc/multipath-tools/examples` e al database multipathd in uso:

```
# echo 'show config' | multipathd -k > multipath.conf-live
```

Per ovviare a una particolarità in multipathd, quando un `/etc/multipath.conf` non esiste, il precedente comando non restituisce nulla, in quanto è il risultato di una *unione* fra il `/etc/multipath.conf` e il database in memoria. Per rimediare a ciò, occorre definire un file `/etc/multipath.conf` vuoto, utilizzando **touch**, oppure crearne uno che ridefinisca un valore predefinito del tipo:

```
defaults {
user_friendly_names no
}
```

e riavviare multipathd:

```
# service multipath-tools restart
```

Ora il comando «show config» restituirà il database in uso.

3.2. Installazione con il supporto Multipath

Per abilitare il *supporto di multipath durante l'installazione*[1], usare

```
install disk-detect/multipath/enable=true
```

[1] http://wiki.debian.org/DebianInstaller/MultipathSupport

al prompt del programma di installazione. I dispositivi multipath trovati vengono visualizzati come **/dev/mapper/mpath<X>** durante l'installazione.

3.3. Ignorare i dischi locali durante la generazione dei dispositivi multipath

Alcune macchine presentano schede SCSI locali per i propri dischi interni; non è consigliato utilizzare DM-Multipath per i suddetti dispositivi. La seguente procedura mostra come modificare il file di configurazione multipath in modo da ignorare i dischi locali durante la configurazione di multipath.

1. Determinare quali dischi sono interni contrassegnandoli in modo da inserirli nella blacklist. In questo esempio, **`/dev/sda`** è il disco interno. Da notare che come originariamente configurato nel file di configurazione multipath predefinito, l'esecuzione di **multipath -v2** visualizza il disco locale, **/dev/sda** all'interno della mappa di multipath. Per ulteriori informazioni, **multipath**, consultare la sezione *Output del comando multipath*.

```
# multipath -v2
create: SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1 undef WINSYS,SF2372
size=33 GB features="0" hwhandler="0" wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 0:0:0:0 sda 8:0 [---------

device-mapper ioctl cmd 9 failed: Invalid argument
device-mapper ioctl cmd 14 failed: No such device or address
create: 3600a0b80001327d80000006d43621677 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:0 sdb 8:16 undef ready running
    `- 3:0:0:0 sdf 8:80 undef ready running

create: 3600a0b80001327510000009a436215ec undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:1 sdc 8:32 undef ready running
    `- 3:0:0:1 sdg 8:96 undef ready running

create: 3600a0b80001327d800000070436216b3 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:2 sdd 8:48 undef ready running
    `- 3:0:0:2 sdg 8:112 undef ready running

create: 3600a0b80001327510000009b4362163e undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:3 sdd 8:64 undef ready running
    `- 3:0:0:3 sdg 8:128 undef ready running
```

2. Per evitare che il device mapper esegua la mappatura di **/dev/sda** nelle proprie mappe multipath, modificare la sezione della blacklist del file `/etc/multipath.conf` in modo da includere questo dispositivo. Anche se è possibile inserire nella blacklist il dispositivo **sda** utilizzando un tipo

di **devnode**, tale procedura non risulterà sicura poichè **/dev/sda** potrebbe non essere uguale al momento del riavvio. Per inserire nella blacklist singoli dispositivi, utilizzare il WWID del dispositivo in questione. Da notare che all'interno dell'output del comando **multipath -v2**, il WWID del dispositivo `/dev/sda` è SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1. Per inserire nella blacklist questo dispositivo, includere quanto segue nel file `/etc/multipath.conf`.

```
blacklist {
wwid SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1
}
```

3. Dopo aver aggiornato il file `/etc/multipath.conf`, è necessario indicare manualmente al demone **multipathd** di ricaricare il file; il seguente comando ricarica il file `/etc/multipath.conf` aggiornato.

```
# service multipath-tools reload
```

4. Eseguire il seguente comando per rimuovere il dispositivo multipath:

```
# multipath -f SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1
```

5. Per controllare se la rimozione del dispositivo è avvenuta, eseguire il comando **multipath -ll** per visualizzare l'attuale configurazione multipath. Per informazioni sul comando **multipath -ll**, consultare la sezione *Interrogazioni multipath con comandi multipli*.Per controllare che il dispositivo inserito nella blacklist non sia stato aggiunto, eseguire il comando multipath, come nel seguente esempio. Il comando multipath imposta in modo predefinito la prolissità a un livello di **v2** se non viene specificata un'opzione **-v**.

```
# multipath

create: 3600a0b80001327d80000006d43621677 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:0 sdb 8:16 undef ready running
    `- 3:0:0:0 sdf 8:80 undef ready running

create: 3600a0b80001327510000009a436215ec undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:1 sdc 8:32 undef ready running
    `- 3:0:0:1 sdg 8:96 undef ready running

create: 3600a0b80001327d800000070436216b3 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:2 sdd 8:48 undef ready running
    `- 3:0:0:2 sdg 8:112 undef ready running

create: 3600a0b80001327510000009b4362163e undef WINSYS,SF2372
```

```
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
     |- 2:0:0:3 sdd 8:64 undef ready running
       `- 3:0:0:3 sdg 8:128 undef ready running
```

3.4. Configurare i dispositivi di archiviazione

Per impostazione predefinita, DM-Multipath include il supporto per i più comuni array di archiviazione che supportano DM-Multipath. I valori di configurazione predefiniti, inclusi i dispositivi supportati, possono essere trovati nel file `multipath.conf.defaults`.

Se è necessario aggiungere un dispositivo di archiviazione non supportato per impostazione predefinita come dispositivo multipath conosciuto, modificare il file`/etc/multipath.conf` e inserire le appropriate informazioni del dispositivo.

Per esempio, per aggiungere informazioni sulle serie HP Open-V, la voce è simile alla seguente, in cui **%n** è il nome del dispositivo:

```
devices {
     device {
            vendor "HP"
            product "OPEN-V."
            getuid_callout "/lib/udev/scsi_id --whitelisted --device=/dev/%n"
     }
}
```

Per ulteriori informazioni sulla sezione del file di configurazione sui dispositivi, consultare la sezione *File di configurazione - dispositivi [72]*.

4. Il file di configurazione DM-Multipath

Per impostazione predefinita, DM-Multipath fornisce i valori di configurazione per gli utilizzi più comuni di multipath. In aggiunta, DM-Multipath include il supporto per i più comuni array di archiviazione che supportano DM-Multipath. I valori di configurazione predefiniti e i dispositivi supportati sono disponibili all'interno del file `multipath.conf.defaults`.

È possibile sovrascrivere i valori di configurazione predefiniti per DM-Multipath modificando il file di configurazione `/etc/multipath.conf`. Se necessario, è possibile aggiungere al file di configurazione un array di archiviazione non supportato per impostazione predefinita. Questo capitolo fornisce informazioni su come analizzare e modificare il file `multipath.conf`, e contiene altresì sezioni relative ai seguenti argomenti:

Nel file di configurazione di multipath devono essere specificate solo le sezioni necessarie per la configurazione o che devono essere modificate rispetto ai valori predefiniti specificati nel file `multipath.conf.defaults`. Se sono presenti sezioni del file non rilevanti per il proprio ambiente o per i quali non devono essere sovrascritti i valori predefiniti, è possibile lasciarli decommentati, come riportato nel file iniziale.

Il file di configurazione permette una sintassi regolare nella descrizione dell'espressione.

Una versione commentata del file di configurazione è disponibile in `/usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz`.

4.1. Panoramica sul file di configurazione

Il file di configurazione di multipath è suddiviso nelle seguenti sezioni:

blacklist
: Un elenco di dispositivi specifici che non verranno considerati per multipath.

blacklist_eccezioni
: Elenco dei candidati di multipath che altrimenti verrebbero inseriti nella blacklist in base ai parametri della sezione relativa.

impostazioni predefinite
: Impostazioni predefinite generali per DM-Multipath.

multipath
: Impostazioni per le caratteristiche dei dispositivi multipath individuali; questi valori sovrascrivono i valori specificati nelle sezioni **defaults** e **devices** del file di configurazione.

dispositivi

Impostazioni per i controller individuali di archiviazione; questi valori sovrascrivono i valori specificati nella sezione **defaults** del file di configurazione. Se si usa un array di archiviazione non supportato in modo predefinito, è necessario creare una sottosezione dispositivi per il proprio array.

Quando il sistema determina gli attributi di un dispositivo multipath, controlla prima le impostazioni di multipath, successivamente le impostazioni di ogni dispositivo e quindi i valori predefiniti del sistema multipath.

4.2. File di configurazione - blacklist

La sezione blacklist del file di configurazione multipath specifica i dispositivi che non verranno utilizzati quando il sistema configura i dispositivi multipath. I dispositivi presenti all'interno della blacklist non verranno raggruppati all'interno di un dispositivo multipath.

- Se è necessario inserire dispositivi nella blacklist, seguire i seguenti criteri:
  - Per WWID, come descritto in *Inserimento nella blacklist in base al WWID [64]*
  - Per nome del dispositivo, come descritto in *Inserimento nella blacklist in base al nome del dispositivo [64]*
  - Per tipo di dispositivo, come descritto in *Inserimento nella blacklist in base al tipo di dispositivo [65]*

  Per impostazione predefinita, anche dopo aver decommentato la sezione iniziale della blacklist del file di configurazione, una serie di dispositivi è inserita nella blacklist. Per ulteriori informazioni, consultare *Inserimento nella blacklist in base al nome del dispositivo [64]*

4.2.1. Inserimento nella blacklist in base al WWID

È possibile specificare i dispositivi individuali da inserire nella blacklist tramite il loro World-Wide IDentification, attraverso una voce **wwid** nella sezione **blacklist** del file di configurazione.

Il seguente esempio mostra le righe all'interno del file di configurazione in grado di inserire in blacklist un dispositivo con un WWID di 26353900f02796769.

```
blacklist {
       wwid 26353900f02796769
}
```

4.2.2. Inserimento nella blacklist in base al nome del dispositivo

È possibile inserire nella blacklist i tipi di dispositivi in base al nome, in modo tale da non farli raggruppare all'interno di un dispositivo multipath, per mezzo di una voce **devnode** nella sezione **blacklist** del file di configurazione.

Il seguente esempio mostra le righe usate nel file di configurazione per inserire nella blacklist tutti i dispositivi SCSI, poichè comprende tutti i dispositivi sd*.

```
blacklist {
       devnode "^sd[a-z]"
}
```

È possibile usare una voce **devnode** nella sezione **blacklist** del file di configurazione, per specificare i dispositivi individuali da inserire nella blacklist, invece di specificare tutti i dispositivi di una tipologia ben precisa; tuttavia questa procedura non è consigliata. A meno che non sia mappato staticamente dalle regole udev, non vi è alcuna garanzia che un dispositivo specifico avrà lo stesso nome al momento del riavvio. Per esempio, un nome del dispositivo potrebbe cambiare da `/dev/sda` a `/dev/sdb`.

Per impostazione predefinita, le seguenti voci **devnode** sono compilate nella blacklist predefinita; i dispositivi che queste voci inseriscono in blacklist generalmente non supportano DM-Multipath. Per abilitare il multipath di uno di questi dispositivi, è necessario specificarlo nella sezione **blacklist_exceptions** del file di configurazione, come descritto in *Eccezioni della blacklist [65]*

```
blacklist {
       devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
       devnode "^hd[a-z]"
}
```

4.2.3. Inserimento nella blacklist in base al tipo di dispositivo

È possibile specificare tipi di dispositivi specifici nella sezione **blacklist** del file di configurazione con una sezione «device». Nel seguente esempio vengono inseriti nella blacklist tutti i dispositivi IBM DS4200 e HP.

```
blacklist {
       device {
               vendor "IBM"
               product "3S42" #DS4200 Product 10
       }
       device {
               vendor "HP"
               product "*"
       }
}
```

4.2.4. Eccezioni della blacklist

È possibile usare la sezione **blacklist_exceptions** del file di configurazione per abilitare il multipath dei dispositivi che sono stati inseriti nella blacklist per impostazione predefinita.

Per esempio, se è presente un gran numero di dispositivi ed è necessario effettuare il multipath di solo uno di essi (con un WWID di 3600d0230000000000e13955cc3757803), invece di inserire individualmente in blacklist tutti i dispositivi tranne quello sul quale effettuare il multipath, è

possibile inserirli tutti in blacklist, e poi consentire il multipath di quello sopra indicato inserendo le seguenti righe nel file `/etc/multipath.conf` file.

```
blacklist {
        wwid "*"
}

blacklist_exceptions {
        wwid "3600d0230000000000e13955cc3757803"
}
```

Quando vengono specificati i dispositivi all'interno della sezione **blacklist_exceptions** del file di configurazione, è necessario specificare le eccezioni nello stesso modo in cui sono state specificate all'interno della **blacklist**. Per esempio, una eccezione WWID non sarà applicata ai dispositivi specificati con una voce della blacklist **devnode**, anche se il dispositivo in blacklist è associato con quel WWID. Allo stesso modo, le eccezioni devnode sono applicate solo alle voci devnode, e le eccezioni device sono applicate solo alle voci device.

4.3. Impostazioni predefinite del file di configurazione

Il file di configurazione `/etc/multipath.conf` comprende una sezione **defaults** che imposta il parametro **user_friendly_names** su **yes** nel modo seguente.

```
defaults {
        user_friendly_names yes
}
```

Ciò sovrascrive il valore predefinito del parametro **user_friendly_names**.

Il file di configurazione include un modello delle impostazioni predefinite della configurazione. Questa sezione è decommentata nel modo seguente.

```
#defaults {
# udev_dir /dev
# polling_interval 5
# selector "round-robin 0"
# path_grouping_policy failover
# getuid_callout "/lib/dev/scsi_id --whitelisted --device=/dev/%n"
# prio   const
# path_checker  directio
# rr_min_io  1000
# rr_weight  uniform
# failback  manual
# no_path_retry  fail
# user_friendly_names no
#}
```

Per sovrascrivere il valore predefinito per qualsiasi parametro di configurazione, è possibile copiare la riga rilevante da questo modello all'interno della sezione **defaults** decommentandola. Per esempio, per sovrascrivere il parametro **path_grouping_policy**in modo da avere **multibus** invece del valore predefinito di **failover**, copiare la riga appropriata dal modello nella sezione iniziale **defaults** del file di configurazione e decommentarla nel modo seguente.

```
defaults {
        user_friendly_names yes
        path_grouping_policy multibus
}
```

La tabella *Configurazione predefinita del multipath [67]* descrive gli attributi impostati nella sezione **defaults** del file di configurazione `multipath.conf`. Questi valori sono utilizzati da DM-Multipath a meno che non siano sovrascritti dagli attributi specificati nelle sezioni **devices** e **multipaths** del file `multipath.conf`.

Tabella 5.2. Configurazione predefinita del multipath

Attributo	**Descrizione**
polling_interval	Specifica l'intervallo, espresso in secondi, fra due controlli del percorso. Per percorsi che operano correttamente, l'intervallo fra controlli aumenterà progressivamente (4 * **polling_interval**); il valore predefinito è **5**.
udev_dir	La directory dove sono creati i nodi del dispositivo udev; il valore predefinito è /dev.
multipath_dir	La directory dove vengono archiviati gli oggetti condivisi dinamici; il valore predefinito dipende dal sistema, in genere `/lib/multipath`.
verbosity	La prolissità predefinita; i valori più elevati aumentano il livello di prolissità. Sono ammessi valori fra 0 e 6, il valore predefinito è 2.
path_selector	Specifica l'algoritmo predefinito da usare per determinare il percorso da utilizzare per l'operazione I/O successiva. Possibili valori includono: • **round-robin 0**: Esegue un loop attraverso ogni percorso nel gruppo di percorso, inviando la stessa quantità di I/O a ognuno di essi. • **queue-length 0**: invia il gruppo successivo di I/O al percorso con il numero minore di richieste I/O pendenti. • **service-time 0**: invia il gruppo successivo di I/O al percorso con il tempo di servizio stimato più breve, determinato dividendo la dimensione totale di I/O pendenti per ogni percorso per il carico di lavoro relativo. Il valore predefinito è **round-robin 0**.

Attributo	**Descrizione**
path_grouping_policy	Specifica la politica predefinita per il gruppo di percorso da applicare ai multipath non specificati. I possibili valori includono: • **failover** = 1 percorso per ogni gruppo di priorità • **multibus** = tutti i percorsi validi in 1 gruppo di priorità • **group_by_serial** = 1 gruppo di priorità per numero seriale rilevato • **group_by_prio** = 1 gruppo di priorità per valore di priorità del percorso • **group_by_node_name** = 1 gruppo di priorità per nome del nodo di destinazione. Il valore predefinito è **failover**.
getuid_callout	Specifica il programma predefinito e gli argomenti da invocare per ottenere un identificatore univoco del percorso; è necessario un percorso assoluto. Il valore predefinito è **/lib/udev/scsi_id --whitelisted --device=/dev/%n**.
prio	Specifica la funzione predefinita da invocare per ottenere un valore per la priorità del percorso; per esempio, i bit ALUA in SPC-3 forniscono un valore sfruttabile di priorità. Possibili valori includono: • **const**: imposta una priorità uguale a 1 per tutti i percorsi. • **emc**: genera la priorità del percorso per gli array EMC. • **alua**: genera la priorità del percorso in base alle impostazioni SCSI-3 ALUA. • **netapp**: genera la priorità del percorso per gli array NetApp. • **rdac**: genera la priorità del percorso per il controller LSI/Engenio RDAC. • **hp_sw**: genera la priorità del percorso per il controller Compaq/HP in modalità attiva/standby. • **hds**: genera la priorità del percorso per gli array di archiviazione modulari Hitachi HDS. Il valore predefinito è **const**.
prio_args	La stringa di argomenti passata alla funzione prio; molte funzioni prio non necessitano di argomenti. Per l'assegnatore di priorità datacore ne serve uno, per esempio **"timeout=1000 preferredsds=foo"**. Il valore predefinito è **""** (null).
caratteristiche	Le funzioni aggiuntive predefinite dei dispositivi multipath. La sola funzione esistente è **queue_if_no_path**, la quale risulta equivalente

Attributo	Descrizione
	all'impostazione **no_path_retry** su **queue**. Per informazioni sui possibili problemi durante l'utilizzo, consultare la sezione *«Problemi con la caratteristica queue_if_no_path»*.
path_checker	Specifica il metodo predefinito usato per determinare lo stato dei percorsi. I possibili valori includono: • **readsector0**: legge il primo settore del dispositivo. • **tur**: emette un TEST UNIT READY per il dispositivo. • **emc_clariion**: interroga 0xC0 della pagina EVPD specifica EMC Clariion per determinare il percorso. • **hp_sw**: controlla lo stato del percorso per gli array di archiviazione HP con firmware Attivo/Standby. • **rdac**: controlla le statistiche del percorso per il controller di archiviazione LSI/Engenio RDAC. • **directio**: legge il primo settore con I/O diretto. Il valore predefinito è **directio**.
failback	Gestisce il failback del gruppo di percorso. • Un valore **immediate** specifica un failback immediato sul gruppo di percorso con la priorità più alta che contiene percorsi attivi. • Un valore **manual** specifica che non ci deve essere un failback immediato ma tale operazione si deve verificare solo attraverso un intervento dell'operatore. • Un valore numerico maggiore di zero specifica un rinvio del failback, espresso in secondi. Il valore predefinito è **manual**.
rr_min_io	Specifica il numero di richieste I/O da indirizzare a un percorso, prima di passare al percorso successivo all'interno del gruppo di percorsi corrente.
rr_weight	Se impostato su **priorities**, invece di eseguire l'invio delle richieste **rr_min_io** a un percorso prima di indicare a **path_selector** di selezionare il percorso successivo, determina il numero di richieste da inviare in base a **rr_min_io** moltiplicato per il valore della priorità del percorso, come determinato dalla funzione prio. Se impostato su **uniform**, tutti i pesi del percorso sono uguali. Il valore predefinito è **uniform**.
no_path_retry	Un valore numerico per questo attributo specifica il numero di volte che il sistema dovrebbe cercare di utilizzare un percorso fallito prima di

Attributo	Descrizione
	disabilitarne la coda. Un valore «fail» indica un fallimento **immediato**, senza accodamento. Un valore **queue** indica che l'accodamento non deve essere arrestato fino a quando il percorso non è stato corretto.
user_friendly_names	Se impostato su «yes», specifica che il sistema deve utilizzare il file `/etc/multipath/bindings` per assegnare un **alias** unico e persistente al **multipath**, con un formato mpathn. Se impostato su «no», specifica che il sistema deve usare il WWID come **alias** per il **multipath**. In entrambi i casi qualsiasi cosa venga specificata sarà sovrascritta da qualsiasi alias specifico per il dispositivo specificato nella sezione multipath del file di configurazione. Il valore predefinito è **«no»**.
queue_without_daemon	Se impostato su «no», il demone **multipathd** disabiliterà l'accodamento di tutti i dispositivi quando viene arrestato. Il valore predefinito è **«yes»**.
flush_on_last_del	Se impostato su «yes», **multipath** disabiliterà l'accodamento quando l'ultimo percorso per un dispositivo è stato cancellato. Il valore predefinito è **«no»**.
max_fds	Imposta il numero massimo di descrittori di file che possono essere aperti da **multipath** e dal demone **multipathd**. Ciò è equivalente al comando ulimit -n. Un valore «max» imposterà tale valore sul limite del sistema di `/proc/sys/fs/nr_open`. Se non impostato, il numero massimo di descrittori viene preso dal processo che esegue la chiamata; generalmente questo valore è 1024. A tale scopo si consiglia di impostare tale valore sul numero massimo di percorsi più 32, se tale numero è maggiore di 1024.
checker_timer	Il timeout da usare per i controllori del percorso che emettono i comandi SCSI con un timeout esplicito, in secondi. Il valore predefinito viene preso da `/sys/block/sdx/device/timeout` ed è uguale a `30` secondi in 12.04 LTS
fast_io_fail_tmo	Il numero di secondi di attesa del livello SCSI dopo il rilevamento di un problema su di una porta remota FC prima di interrompere gli I/O per i dispositivi di quella porta remota. Questo valore deve essere minore del valore dev_loss_tmo; l'impostazione su «off» disabiliterà il timeout. Il valore predefinito viene determinato dal sistema operativo.
dev_loss_tmo	Il numero di secondi di attesa del livello SCSI dopo il rilevamento di un problema su di una porta remota FC prima di rimuoverlo dal sistema;

Attributo	Descrizione
	l'impostazione a «infinity» porterà l'intervallo a 2147483647 secondi, o 68 anni. Il valore predefinito è determinato dal sistema operativo.

4.4. Attributi del file di configurazione di multipath

La tabella *Attributi di multipath [71]* mostra gli attributi da impostare nella sezione **multipaths** del file di configurazione `multipath.conf` per ciascun specifico dispositivo multipath; questi attributi vengono applicati solo a quel multipath specificato. Queste impostazioni predefinite sono utilizzate da DM-Multipath e sovrascrivono gli attributi impostati nelle sezioni **defaults** e **devices** del file di configurazione multipath.conf.

Tabella 5.3. Attributi di multipath

Attributo	Descrizione
wwid	Specifica il WWID del dispositivo **multipath** al quale sono applicabili gli attributi **multipath**. Questo parametro è obbligatorio per questa sezione del file `multipath.conf`.
alias	Specifica il nome simbolico per il dispositivo **multipath** al quale sono applicabili gli attributi **multipath**. Se si usano **user_friendly_names**, non impostare questo valore su mpathn; tale impostazione può entrare in conflitto con un nome descrittivo assegnato automaticamente, generando nomi del nodo del dispositivo non corretti.

In aggiunta, i seguenti parametri possono essere sovrascritti in questa sezione **multipath**

- *`path_grouping_policy`*
- *`path_selector`*
- *`failback`*
- *`prio`*
- *`prio_args`*
- *`no_path_retry`*
- *`rr_min_io`*
- *`rr_weight`*
- *`flush_on_last_del`*

Il seguente esempio mostra gli attributi multipath specificati nel file di configurazione per due specifici dispositivi multipath. Il primo dispositivo presenta un WWID di 3600508b4000156d70001200000b0000 e il nome simbolico «giallo».

Il secondo dispositivo multipath nell'esempio ha un WWID di 1DEC_____321816758474 e il nome simbolico «rosso»; in questo esempio, l'attributo *rr_weight* è impostato su «priorities».

```
multipaths {
       multipath {
              wwid 3600508b4000156d70001200000b0000
              alias giallo
              path_grouping_policy multibus
              path_selector "round-robin 0"
              failback manual
              rr_weight priorities
              no_path_retry 5
       }
       multipath {
              wwid 1DEC_____321816758474
              alias rosso
              rr_weight priorities
       }
}
```

4.5. File di configurazione - dispositivi

La tabella *Attributi del dispositivo [73]* mostra gli attributi che possono essere impostati per ogni singolo dispositivo di archiviazione nella sezione «device» del file di configurazione multipath.conf; questi attributi sono utilizzati da DM-Multipath a meno che non siano sovrascritti dagli attributi specificati nella sezione **multipaths** del file `multipath.conf` per i percorsi che contengono il dispositivo. Questi attributi sovrascrivono quelli impostati nella sezione **defaults** del file `multipath.conf`.

Numerosi dispositivi che supportano il multipath sono inclusi per impostazione predefinita in una configurazione multipath; i valori per i dispositivi supportati per impostazione predefinita sono elencati nel file `multipath.conf.defaults`. Molto probabilmente non sarà necessario modificare i valori per questi dispositivi, ma se fosse necessario farlo sarà possibile sovrascrivere i valori predefiniti includendo una voce nel file di configurazione per il dispositivo che sovrascrive questi valori. È possibile copiare la configurazione predefinita per il dispositivo dal file `multipath.conf.annotated.gz` o, se è necessario avere un file di configurazione sintetico, dal file `multipath.conf.synthetic` e sovrascrivere i valori da modificare.

Per aggiungere un dispositivo in questa sezione del file di configurazione non configurata automaticamente per impostazione predefinita, sarà necessario impostare i parametri **vendor** e **product**. Questi valori sono disponibili su **/sys/block/device_name/device/vendor** e **/sys/block/device_name/device/model**, dove device_name è il dispositivo sul quale eseguire il multipath, come riportato nel seguente esempio:

```
# cat /sys/block/sda/device/vendor
WINSYS
# cat /sys/block/sda/device/model
SF2372
```

Gli ulteriori parametri da specificare dipendono dallo specifico dispositivo: se questo è ativo/attivo, normalmente non è necessario impostare parametri aggiuntivi; può essere necessario impostare

path_grouping_policy su **multibus**. Altri parametr i da impostare possono essere *no_path_retry* e *rr_min_io*, come descritto nella tabella *Attributi di multipath [71]*.

Se il dispositivo è attivo/passivo, ma smista automaticamente il percorso con I/O sul percorso passivo, è necessario modificare la funzione del controller su una funzione non in grado d'inviare alcun segnale I/O al percorso per controllarne il suo funzionamento (in caso contrario il dispositivo continuerà a eseguire un failover). Ciò quasi sempre significa impostare *path_checker* su **tur**; questo processo funziona per tutti i dispositivi SCSI che supportano il comando Test Unit Ready, cosa che molti fanno.

Se il dispositivo necessita di un comando speciale per smistarsi da un percorso ad un altro, allora la configurazione di questo dispositivo per multipath richiederà un modulo del kernel gestore hardware. Il gestore hardware attuale è emc; se non è sufficiente per il dispositivo, allora non sarà possibile configurare il dispositivo per il multipath.

Tabella 5.4. Attributi del dispositivo

Attributo	Descrizione
fornitore	Specifica il nome del fornitore del dispositivo di archiviazione sul quale sono applicabili gli attributi del dispositivo, per esempio **COMPAQ**.
prodotto	Specifica il nome del prodotto del dispositivo di archiviazione sul quale sono applicabili gli attributi del dispositivo, per esempio **HSV110 (C)COMPAQ**.
revisione	Specifica l'identificatore della revisione del prodotto del dispositivo di archiviazione.
product_blacklist	Specifica un'espressione regolare usata per inserire nella blacklist i dispositivi in base al prodotto.
hardware_handler	Specifica un modulo che verrà utilizzato per eseguire le azioni hardware specifiche, quando si esegue lo smistamento dei gruppi di percorso o di gestione degli errori I/O. I possibili valori includono: • **1 emc**: gestore hardware di array di archiviazione EMC. • **1 alua**: gestore hardware per array SCSI-3 ALUA. • **1 hp_sw**: gestore hardware per controller Compaq/HP. • **1 rdac**: gestore hardware per controller LSI/Engenio RDAC.

Oltre a ciò, è possibile sovrascrivede i seguenti parametri in questa sezione **device**

- `path_grouping_policy`
- `getuid_callout`
- `path_selector`
- `path_checker`

- *caratteristiche*
- *failback*
- *prio*
- *prio_args*
- *no_path_retry*
- *rr_min_io*
- *rr_weight*
- *fast_io_fail_tmo*
- *dev_loss_tmo*
- *flush_on_last_del*

Whenever a hardware_handler is specified, it is your responsibility to ensure that the appropriate kernel module is loaded to support the specified interface. These modules can be found in **/lib/modules/`uname -r`/kernel/drivers/scsi/device_handler/** . The requisite module should be integrated into the initrd to ensure the necessary discovery and failover-failback capacity is available during boot time. Example,

```
# echo scsi_dh_alua >> /etc/initramfs-tools/modules  ## append module to file
# update-initramfs -u -k all
```

Il seguente esempio mostra una voce device nel file di configurazione di multipath.

```
#devices {
# device {
#  vendor   "COMPAQ  "
#  product   "MSA1000         "
#  path_grouping_policy multibus
#  path_checker  tur
#  rr_weight  priorities
# }
#}
```

La spaziatura riservata nei campi **vendor**, **product** e **revision** è significativa per il modo in cui multipath trova una corrispondenza diretta per questi attributi, il cui formato è definito dalla specifica SCSI, precisamente con il comando *Standard INQUIRY*[2]. Quando sono usate le virgolette, i campi vendor, product e revision sono interpretati tassativamente in maniera conforme alla specificazione; all'interno delle stringhe virgolettate possono essere integrate espressioni regolari. Se un campo viene definito senza la spaziatura richiesta, multipath copierà la stringa nel buffer adeguatamente dimensionato, riempiendolo con il corretto numero di spazi. La specifica deve essere popolata da caratteri stampabili o da spazi, come mostrato nel precedente esempio.

- vendor: 8 caratteri
- product: 16 caratteri

[2] http://en.wikipedia.org/wiki/SCSI_Inquiry_Command

- revision: 4 caratteri

Per creare un file di configurazione più robusto, è possibile usare anche espressioni regolari; gli operatori includono **^ $ [ ] . * ? +**. Esempi di espressioni regolari funzionanti possono essere trovati esaminando il database multipath in uso e file di esempio di `multipath.conf` possono essere trovati in `/usr/share/doc/multipath-tools/examples`:

```
# echo 'show config' | multipathd -k
```

5. Amministrazione e risoluzione di problemi di DM-Multipath

5.1. Ridimensionare un dispositivo multipath online

Per ridimensionare un dispositivo multipath online, usare la seguente procedura.

1. Ridimensionare il dispositivo fisico: questo è specifico per una piattaforma di archiviazione.
2. Usare il seguente comando per trovare i percorsi del LUN:

```
# multipath -l
```

3. Ridimensionare i percorsi; per i dispositivi SCSI, l'inserimento di 1 nel file `rescan` per il dispositivo causa una nuova scansione da parte del driver SCSI, come nel seguente comando:

```
# echo 1 > /sys/block/device_name/device/rescan
```

4. Ridimensionare il dispositivo multipath eseguendo il comando multipathd resize:

```
# multipathd -k 'resize map mpatha'
```

5. Ridimensionare il file system (assumendo che non siano usate partizioni LVM o DOS):

```
# resize2fs /dev/mapper/mpatha
```

5.2. Spostare i file system root da un dispositivo a percorso singolo a un dispositivo multipath.

Ciò è drasticamente semplificato dall'utilizzo degli UUID per identificare i dispositivi come un'etichetta intrinseca: basta installare **multipath-tools-boot** e riavviare. Questo ricostruisce il ramdisk iniziale e consente a multipath l'opportunità di costurire i propri percorsi prima che il file system root sia montato dall'UUID.

Ogni qualvolta `multipath.conf` viene aggiornato, lo stesso deve essere fatto con initrd eseguendo il comando **update-initramfs -u -k all**; questo perchè `multipath.conf` viene copiato nel ramdisk ed è parte integrante nella determinazione dei dispositivi disponibili per il raggruppamento tramite la sua blacklist e le sezioni device.

5.3. Spostare i file system di swap da un dispositivo a percorso singolo a un dispositivo multipath

La procedura è esattamente la stessa di quella illustrata nella precedente sezione chiamata *Spostare i file system root da un dispositivo a percorso singolo a un dispositivo multipath*.

5.4. Il demone di multipath

In caso di problemi nell'implementare una configurazione multipath, è necessario assicurarsi che il demone multipath sia in esecuzione come descritto in *Impostare DM-Multipath*. Per usare i dispositivi multipathd è necessario che il demone **multipathd** sia in esecuzione. Consultare anche la sezione

Risoluzione di problemi con la console interattiva multipathd relativa all'interazione con **multipathd** come aiuto al debug.

5.5. Problemi con queue_if_no_path

Se **features "1 queue_if_no_path"** è stato specificato nel file `/etc/multipath.conf`, qualsiasi processo che emette I/O si arresterà fino a quando non verranno ripristinati uno o più percorsi. Per evitare questo problema, impostare il parametro ***no_path_retry*** **N** in `/etc/multipath.conf`.

Quando si imposta il parametro **no_path_retry**, è necessario rimuovere l''opzione **features "1 queue_if_no_path"** dal file `/etc/multipath.conf`. Se tuttavia viene usato un dispositivo multipath per il quale è stata impostata in modo predefinito l'opzione `features "1 queue_if_no_path"`, come nel caso di numerosi dispositivi SAN, è necessario aggiungere `features "0"` per sovrascrivere l'impostazione predefinita. Per tale operazione copiare la sezione esistente **devices**, solo la sezione e non l'intero file, da `/usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz` in `/etc/multipath.conf` modificandolo in base alle proprie esigenze. esistenti per il dispositivo da

Se è necessario utilizzare l'opzione `features "1 queue_if_no_path"` e si è riscontrato il problema qui riportato, usare il comando **dmsetup** per modificare la politica al momento dell'esecuzione per un LUN specifico (cioè, per il quale tutti i percorsi risultano non disponibili). Per esempio, se si desidera modificare la politica sul dispositivo multipath `mpathc` da `"queue_if_no_path"` a `"fail_if_no_path"`, eseguire il seguente comando.

```
# dmsetup message mpathc 0 "fail_if_no_path"
```

È necessario specificare l'alias `mpathN` e non il percorso.

5.6. Output del comando Multipath

Quando viene creato, modificato o elencato un dispositivo multipath, si riceve una stampa sull'impostazione corrente del dispositivo; il formato è il seguente, per ciascun dispositivo multipath:

```
action_if_any: alias (wwid_if_different_from_alias) dm_device_name_if_known vendor,product
size=size features='features' hwhandler='hardware_handler' wp=write_permission_if_known
```

Per ogni gruppo del percorso:

```
-+- policy='scheduling_policy' prio=prio_if_known
status=path_group_status_if_known
```

Per ogni percorso:

```
 `- host:channel:id:lun devnode major:minor dm_status_if_known path_status
online_status
```

Per esempio, l'output di un comando multipath potrebbe apparire nel modo seguente:

```
3600d0230000000000e13955cc3757800 dm-1 WINSYS,SF2372
size=269G features='0' hwhandler='0' wp=rw
```

```
  |-+- policy='round-robin 0' prio=1 status=active
  | `- 6:0:0:0 sdb 8:16 active ready running
  `-+- policy='round-robin 0' prio=1 status=enabled
    `- 7:0:0:0 sdf 8:80 active ready running
```

Se il percorso è attivo ed è pronto per l'I/O, lo stato del percorso è **ready** o *ghost*. Se il percorso non è attivo, lo stato è **faulty** o **shaky**. Lo stato del percorso viene aggiornato periodicamente dal demone **multipathd** in base all'intervallo di interrogazione definito nel file `/etc/multipath.conf`.

Lo stato relativo a dm è simile allo stato del percorso, ma dal punto di vista del kernel; esso presenta due opzioni: **failed**, analogo a **faulty** e **active**, che interessa tutti gli altri stati del percorso. Occasionalmente lo stato del percorso e quello dm di un dispositivo possono non corrispondere temporaneamente.

I valori possibili per **online_status** sono **running** e **offline**. Uno stato di *offline* significa che il dispositivo SCSI è stato disabilitato.

Quando un dispositivo multipath è stato creato o modificato, lo stato del gruppo del percorso, il nome dm del dispositivo, i permessi di scrittura e lo stato dm non sono conosciuti. In aggiunta, le caratteristiche non sono sempre corrette.

5.7. Interrogazioni multipath con il comando multipath

È possibile utilizzare le opzioni **-l** e **-ll** del comando **multipath** per visualizzare la configurazione corrente di multipath. L'opzione **-l** visualizza la topologia di multipath in base alle informazioni in sysfs e del device mapper. L'opzione **-ll** visualizza le informazioni mostrate da **-l** insieme ad altri componenti disponibili del sistema.

Durante la visualizzazione della configurazione di multipath, è possibile specificare con l'opzione **-v** tre livelli di prolissità del comando multipath. Specificando **-v0**, non verrà riprodotto alcun output; specificando **-v1** verranno visualizzati solo i nomi multipath creati o modificati utilizzabili per altri strumenti come per esempio kpartx; specificando **-v2**, verranno visualizzati tutti i percorsi rilevati, i multipath e le mappe del dispositivo.

Il livello di **prolissità** di multipath è **2** ed è possibile modificarlo globalmente definendo la *verbosity attribute* nella sezione **defaults** di `multipath.conf`.

Il seguente esempio mostra l'output di un comando **multipath -l**.

```
# multipath -l
  3600d0230000000000e13955cc3757800 dm-1 WINSYS,SF2372
  size=269G features='0' hwhandler='0' wp=rw
  |-+- policy='round-robin 0' prio=1 status=active
  | `- 6:0:0:0 sdb 8:16 active ready running
  `-+- policy='round-robin 0' prio=1 status=enabled
    `- 7:0:0:0 sdf 8:80 active ready running
```

Il seguente esempio mostra l'output di un comando **multipath -ll**.

```
# multipath -ll
  3600d0230000000000e13955cc3757801 dm-10 WINSYS,SF2372
  size=269G features='0' hwhandler='0' wp=rw
  |-+- policy='round-robin 0' prio=1 status=enabled
  | `- 19:0:0:1 sdc 8:32 active ready running
  `-+- policy='round-robin 0' prio=1 status=enabled
    `- 18:0:0:1 sdh 8:112 active ready running
    3600d0230000000000e13955cc3757803 dm-2 WINSYS,SF2372
    size=125G features='0' hwhandler='0' wp=rw
    `-+- policy='round-robin 0' prio=1 status=active
      |- 19:0:0:3 sde 8:64 active ready running
        `- 18:0:0:3 sdj 8:144 active ready running
```

5.8. Opzioni del comando Multipath

Table *Opzioni utili del comando multipath [79]* describes some options of the **multipath** command that you might find useful.

Tabella 5.5. Opzioni utili del comando multipath

Opzione	Descrizione
-l	Visualizza la configurazione multipath corrente proveniente da **sysfs** e il device mapper.
-ll	Mostra la configurazione multipath corrente proveniente da **sysfs**, il device mapper e tutti gli altri componenti disponibili sul sistema.
-f device	Rimuove il dispositivo multipath indicato.
-F	Rimuove tutti i dispositivi multipath inutilizzati.

5.9. Determinare le voci del Device Mapper con il comando dmsetup

È possibile utilizzare il comando **dmsetup** per sapere quale voce del device mapper corrisponde ai dispositivi sui quali è stato eseguito il **multipath**.

Il seguente comando visualizza tutti i dispositivi del device mapper insieme ai rispettivi numeri maggiori e minori. I numeri minori determinano il nome del dispositivo dm. Per esempio, un numero minore di **3** corrisponde al dispositivo multipath **`/dev/dm-3`**.

```
# dmsetup ls
mpathd (253, 4)
mpathep1 (253, 12)
mpathfp1 (253, 11)
mpathb (253, 3)
mpathgp1 (253, 14)
mpathhp1 (253, 13)
mpatha (253, 2)
mpathh (253, 9)
```

```
mpathg (253, 8)
VolGroup00-LogVol01 (253, 1)
mpathf (253, 7)
VolGroup00-LogVol00 (253, 0)
mpathe (253, 6)
mpathbp1 (253, 10)
mpathd (253, 5)
```

5.10. Risoluzione dei problemi con la console interattiva multipathd

Il comando **multipathd -k** è un'interfaccia interattiva per il demone di **multipathd**; digitando questo comando, viene visualizzata una console di multipath interattiva. Dopo aver inserito questo comando, è possibile digitare help per ottenere un elenco dei comandi disponibili, inserire un comando interattivo o digitare **CTRL-D** per uscire.

La console interattiva di multipathd può essere usata per risolvere i problemi incontrati con il sistema. Per esempio, la seguente sequenza di comandi visualizza la configurazione multipath e le impostazioni predefinite, prima di abbandonare la console. Per ulteriori esempi, consultare l'articolo IBM *Trucchi con multipathd*[3].

```
# multipathd -k
  > > show config
  > > CTRL-D
```

La seguente sequenza di comandi assicura che multipath abbia implementato qualsiasi modifica in multipath.conf.

```
# multipathd -k
> > reconfigure
> > CTRL-D
```

Utilizzare questa sequenza di comandi per assicurarsi che il controllore dei percorsi funzioni correttamente.

```
# multipathd -k
 > > show paths
 > > CTRL-D
```

È possibile riversare i comandi in multipathd usando stdin in questo modo:

```
# echo 'show config' | multipathd -k
```

[3] http://www-01.ibm.com/support/docview.wss?uid=isg3T1011985

Capitolo 6. Amministrazione remota

Ci sono diversi modi per amministrare un server Linux da remoto; questa sezione illustra due dei metodi più comuni, come OpenSSH e Puppet.

1. Server OpenSSH

1.1. Introduzione

Questa sezione della Guida a Ubuntu server introduce una serie di potenti strumenti per il controllo remoto di computer e per il trasferimento di dati tra i computer in rete chiamata *OpenSSH*. Vengono spiegate alcune delle possibili impostazioni dell'applicazione server OpenSSH e come modificarne la configurazione in Ubuntu.

OpenSSH è una versione libera della famiglia di protocolli e strumenti SSH (Secure SHell) per il controllo remoto di un computer o per il trasferimento di file tra computer. Gli strumenti tradizionali usati per svolgere queste funzioni, come telnet o rcp, sono insicuri e quando utilizzati trasmettono la password dell'utente in chiaro. OpenSSH fornisce un demone server e degli strumenti lato client per facilitare operazioni di controllo remoto e trasferimento di file in sicurezza e con crittografia, sostituendo in modo completo gli strumenti tradizionali.

Il componente server di OpenSSH, sshd, è in ascolto continuo per le connessioni in arrivo dei client, qualunque sia lo strumento usato sui client. Quando avviene una richiesta di connessione, per mezzo di sshd viene impostata la corretta connessione in base allo strumento utilizzato dal client. Per esempio, se il computer remoto sta effettuando una connessione con l'applicazione client ssh, il server OpenSSH imposta, dopo l'autenticazione, una sessione di controllo remoto. Se un utente remoto si connette a un server OpenSSH con scp, il demone server OpenSSH inizializza, dopo l'autenticazione, una procedura di copia sicura di file tra il server e il client. OpenSSH permette l'utilizzo di diversi metodi di autenticazione, inclusi password semplice, chiave pubblica e ticket Kerberos.

1.2. Installazione

L'installazione delle applicazioni server e client di OpenSSH è semplice. Per installare l'applicazione client OpenSSH sui sistemi Ubuntu, usare questo comando al prompt di un terminale:

```
sudo apt-get install openssh-client
```

Per installare l'applicazione server di OpenSSH e i relativi file di supporto, usare questo comando al prompt di un terminale:

```
sudo apt-get install openssh-server
```

È possibile scegliere di installare il pacchetto openssh-server durante il processo di installazione della Server Edition.

1.3. Configurazione

È possibile configurare il comportamento predefinito dell'applicazione server di OpenSSH, sshd, modificando il file `/etc/ssh/sshd_config`. Per maggiori informazioni riguardo le direttive di

configurazione usate in questo file, consultare l'appropriata pagina di manuale inserendo, a un prompt di terminale, il seguente comando:

```
man sshd_config
```

All'interno del file di configurazione di sshd sono presenti diverse direttive per controllare impostazioni riguardo la comunicazione o i mezzi di autenticazione. Di seguito vengono riportati degli esempi di direttive di configurazione che è possibile cambiare modificando il file `/etc/ssh/sshd_config`.

Prima di modificare il file di configurazione, è consigliato fare una copia del file originale e proteggerla dalla scrittura, così da avere le impostazioni originali come riferimento ed eventualmente riusarle se necessario.

Copiare il file `/etc/ssh/sshd_config` e proteggerlo da scrittura, con il seguente comando, digitando a un prompt di terminale:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

Quelli che seguono sono esempi delle direttive di configurazione che è possibile cambiare:

- Per impostare OpenSSH in modo da restare in ascolto sulla porta TCP 2222 invece che sulla predefinita porta TCP 22, cambiare la direttiva Port come segue:

  Port 2222

- Per consentire l'utilizzo in sshd di credenziali di accesso basate su chiave pubblica, aggiungere o modificare la riga:

  PubkeyAuthentication yes

  Se la riga è già presente, assicurarsi che non sia commentata.

- Per far sì che il server OpenSSH mostri il contenuto del file `/etc/issue.net` come un banner di pre-accesso, aggiungere o modificare la riga:

  Banner /etc/issue.net

  Nel file `/etc/ssh/sshd_config`.

Dopo aver apportato dei cambiamenti al file `/etc/ssh/sshd_config`, salvarlo e, per rendere effettivi i cambiamenti, riavviare il demone sshd usando il seguente comando:

```
sudo service ssh restart
```

Per poter adattare il comportamento dell'applicazione server alle proprie necessità, sono disponibili molte altre direttive di configurazione per sshd. Se però l'unico metodo per

accedere a un server è ssh, se si commette un errore nella configurazione di sshd attraverso il file `/etc/ssh/sshd_config`, può risultare precluso l'accesso al server dopo il suo riavvio. Inoltre, se viene fornita una direttiva di configurazione non corretta, il server sshd potrebbe non riuscire ad avviarsi; è necessario pertanto prestare grande attenzione nella modifica di questo file su un server remoto.

1.4. Chiavi SSH

Le *chiavi* SSH consentono l'autenticazione tra due host senza la necessità di una password. L'autenticazione con chiave SSH utilizza due chiavi, una *privata* e una *public*.

Per generare le chiavi, in un terminale, digitare:

```
ssh-keygen -t dsa
```

Vengono così generate le chiavi usando un metodo *Digital Signature Algorithm (DSA)*. Durante questo processo viene chiesto di inserire una password: premere semplicemente *Enter* quando viene chiesto di creare la chiave.

La chiave *pubblica* viene salvata, in modo predefinito, nel file `~/.ssh/id_dsa.pub`, mentre quella *privata* in `~/.ssh/id_dsa`. Ora, copiare il file `id_dsa.pub` nell'host remoto e aggiungere il suo contenuto al file `~/.ssh/authorized_keys` digitando:

```
ssh-copy-id NOME_UTENTE@HOST_REMOTO
```

Infine, controllare i permessi del file `authorized_keys`: solo l'utente autenticato dovrebbe avere i permessi di lettura e scrittura. Nel caso non fossero corretti, modificarli:

```
chmod 600 .ssh/authorized_keys
```

Dovrebbe essere possibile ora collegarsi via SSH all'host senza l'utilizzo di una password.

1.5. Riferimenti

- Pagina della *documentazione della comunità su SSH*[1].
- *Sito web di OpenSSH*[2]
- *Pagina wiki di OpenSSH avanzato*[3]

[1] https://help.ubuntu.com/community/SSH
[2] http://www.openssh.org/
[3] https://wiki.ubuntu.com/AdvancedOpenSSH

2. Puppet

Puppet è un'infrastruttura a piattaforma incrociata che consente agli amministratori di sistema di eseguire tramite codice attività comuni, quali l'installazione di nuovo software, il controllo dei permessi sui file o l'aggiornamento di account utente. Puppet è importante non solo durante l'installazione iniziale di un sistema, ma anche attraverso l'intero ciclo di vita del sistema. Puppet viene utilizzato in molte circostanze nella configurazione dei server e dei client.

Questa sezione illustra l'installazione e configurazione di Puppet in una configurazione client/server; questo semplice esempio mostra come installare Apache usando Puppet.

2.1. Installazione

Per installare Puppet, in un terminale sul *server* digitare:

```
sudo apt-get install puppetmaster
```

Sulla macchina, o le macchine, *client*, digitare:

```
sudo apt-get install puppet
```

2.2. Configurazione

Prima di configurare puppet, è necessario aggiungere una voce DNS *CNAME* per *puppet.example.com*, dove *example.com* è il proprio dominio. Per impostazione predefinita, i client Puppet verificano sul DNS che puppet.examnple.com sia il nome del server puppet o il *Puppet Master*. Per maggiori dettagli, consultare *Capitolo 8, DNS (Domain Name Service) [140]*.

Se non si utilizza DNS, è possibile aggiungere delle voci ai file server e client `/etc/hosts`. Per esempio, aggiungere al file `/etc/hosts` del server Puppet:

```
127.0.0.1 localhost.localdomain localhost puppet
192.168.1.17 meercat02.example.com meercat02
```

Su ciascun client Puppet, aggiungere una voce per il server:

```
192.168.1.16 meercat.example.com meercat puppet
```

Sostituire gli indirizzi IP e i nomi di dominio nell'esempio precedente con gli indirizzi e i nomi di dominio reali di server e client.

Impostare quindi alcune risorse per apache2: creare un file `/etc/puppet/manifests/site.pp` contenente quanto segue:

```
package {
    'apache2':
```

```
        ensure => installed
}

service {
    'apache2':
        ensure => true,
        enable => true,
        require => Package['apache2']
}
```

Quindi creare un file `/etc/puppet/manifests/nodes.pp` per il nodo, con:

```
node 'meercat02.example.com' {
   include apache2
}
```

Sostituire *meercat02.example.com* con il nome reale dell'host del client Puppet.

Il passo finale per questo semplice server Puppet consiste nel riavviare il demone:

```
sudo service puppetmaster restart
```

Configurato il server Puppet, è necessario configurare il client.

Per prima cosa, configurare il demone Puppet per l'avvio. Modificare `/etc/default/puppet`, cambiando *START* in «yes»:

```
START=yes
```

Quindi avviare il servizio:

```
sudo service puppet start
```

Tornando sul server Puppet , firmare il certificato client digitando:

```
sudo puppetca --sign meercat02.example.com
```

Controllare il file `/var/log/syslog` per errori di configurazione. Se tutto funziona correttamente, il pacchetto apache2 e le sue dipendenze saranno installati sul client Puppet.

Questo esempio è *molto* semplice e non evidenzia molte delle caratteristiche e dei vantaggi di Puppet. Per ulteriori informazioni, consultare *Sezione 2.3, «Risorse» [86]*.

2.3. Risorse

- Visitare il sito web per consultare la *documentazione ufficiale di Puppet*[4]

[4] http://docs.puppetlabs.com/

- Consultare anche *Pro Puppet*[5].
- Un'altra fonte di ulteriori informazioni è la *pagina della documentazione della comunità di Ubuntu su Puppet*[6].

[5] http://www.apress.com/9781430230571
[6] https://help.ubuntu.com/community/Puppet

3. Zentyal

Zentyal è un server Linux per piccole aziende, che può essere configurato come gateway, gestore d'infrastruttura, gestore unico della sicurezza (Unified Threat Manager), server per ufficio (Office Server), server unico per le comunicazioni (Unified Communication Server) o una combinazione di questi. Tutti i servizi di rete gestiti da Zentyal sono strettamente integrati, rendendo automatici molti processi. Ciò contribuisce a evitare errori nella configurazione e amministrazione della rete e consente di risparmiare tempo. Zentyal è open source, rilasciato sotto licenza GNU (General Public License - GPL) e funziona in ambiente Ubuntu GNU/Linux.

Zentyal consiste di una serie di pacchetti (di solito uno per ciascun modulo) che fornisce un'interfaccia web per configurare i diversi server o servizi. La configurazione è memorizzata in un database chiave-valore Redis ma la configurazione collegata di utenti, gruppi e domini è su OpenLDAP . Quando viene configurato uno dei parametri disponibili attraverso l'interfaccia web, i file finali di configurazione vengono sovrascritti usando i modelli di configurazione forniti dai moduli. I principali vantaggi dell'uso di Zentyal sono: unica interfaccia grafica utente per configurare tutti i servizi di rete ed elevata integrazione fra di essi subito disponibile.

3.1. Installazione

Zentyal 2.3 è disponibile nel repository Universe di Ubuntu 12.04; i moduli disponibili sono:

- zentyal-core e zentyal-common: il cuore dell'interfaccia Zentyal e le librerie comuni dell'infrastruttura. Comprende anche i registri e i moduli di avviso che forniscono all'amministratore un'interfaccia per visualizzare i registri e generano avvisi da questi.
- zentyal-network: gestisce la configurazione della rete. Dalle interfacce (che supportano IP statici, DHCP, VLAN, bridge o PPPoE), ai gateway multipli in caso di più connessioni a internet, bilanciamento dei carichi e istradamento avanzato, rotte statiche o DNS dinamici.
- zentyal-objects e zentyal-services: fornisce un livello di astrazione per indirizzi di rete (per es. LAN invece di 192.168.1.0/24) e porte chiamate come servizi (per es. HTTP invece di 80/TCP).
- zentyal-firewall: configura le regole di iptables per bloccare connessioni proibite, NAT e reindirizzamenti di porte.
- zentyal-ntp: installa il demone NTP per sincronizzare l'orologio software del server e consentire ai client di rete di sincronizzare a loro volta i propri orologi su quello del server.
- zentyal-dhcp: configura un server ISC DHCP che supporta intervalli di rete, indirizzi riservati statici e altre opzioni avanzate come NTP, WINS, aggiornamenti dei DNS dinamici e avvio di rete con PXE.
- zentyal-dns: introduce un server DNS ISC Bind9 nel server per effettuare la cache di query locali in qualità di server d'inoltro o come server autorevole per i domini configurati. Consente di configurare record A, CNAME, MX, NS, TXT e SRV.
- zentyal-ca: integra in Zentyal un gestore di Autorità di Certificazione in modo tale da consentire agli utenti di autenticarsi ai servizi come con OpenVPN.

- zentyal-openvpn: consente di configurare più server e client VPN usando OpenVPN e con configurazione dell'instradamento dinamico tramite Quagga.
- zentyal-users: fornisce un'interfaccia per configurare e gestire utenti e gruppi su OpenLDAP. Altri servizi su Zentyal sono autenticati in LDAP con gestione centralizzata di utenti e gruppi. È anche possibile sincronizzare utenti, password e gruppi da un dominio Microsoft Active Directory.
- zentyal-squid: configura Squid e Dansguardian per aumentare la velocità di navigazione, grazie alle capacità di caching e di filtro dei contenuti.
- zentyal-samba: consente la configurazione di Samba e la sua integrazione con LDAP esistenti. Per mezzo della stessa interfaccia è possibile definire politiche delle password, creare risorse condivise e assegnare permessi.
- zentyal-printers: integra CUPS con Samba e consente non solo di configurare stampanti, ma anche di concedere loro permessi basati su utenti e gruppi LDAP.

Per installare Zentyal, in un terminale sul *server* digitare il seguente comando (in cui «<zentyal-module>» è uno dei moduli dell'elenco precedente):

```
sudo apt-get install <zentyal-module>
```

Zentyal pubblica un principale rilascio stabile una volta all'anno (in settembre) basato sul più recente rilascio LTS di Ubuntu; i rilasci stabili hanno numeri secondari pari (per es. 2.2, 3.0) mentre i rilasci «beta» hanno numeri secondari dispari (per es. 2.1, 2.3). In Ubuntu 12.04 è incluso il pacchetto Zentyal 2.3. Per effettuare il suo aggiornamento a un nuovo rilascio stabile pubblicato dopo il rilascio di Ubuntu 12.04, è possibile usare *Zentyal Team PPA*[7]. L'aggiornamento a un rilascio stabile più recente può fornire correzioni a piccoli bug, non applicate alla versione 2.3 in Precise, e più recenti funzionalità.

If you need more information on how to add packages from a PPA see *Add a Personal Package Archive (PPA)*[8].

In *Zentyal Team PPA*[9] è possibile trovare questi ulteriori moduli, non presenti nei repository di Ubuntu:

- zentyal-antivirus: integra l'antivirus ClamAV con altri moduli come il proxy, la condivisione di file o il filtro di posta.
- zentyal-asterisk: configura Asterisk per fornire un semplice centralino telefonico (PBX, Private Branch Exchange) con autenticazione basata su LDAP.
- zentyal-bwmonitor: consente di monitorare l'uso della banda di rete da parte dei client LAN.
- zentyal-captiveportal: integra un portale di accesso obbligatorio (captive portal) con firewall e utenti e gruppi LDAP.

[7] https://launchpad.net/~zentyal/
[8] https://help.ubuntu.com/$distro-rev-short/ubuntu-help/addremove-ppa.html
[9] https://launchpad.net/~zentyal/

- zentyal-ebackup: consente di effetture backup pianificati del server usando il popolare strumento di backup duplicity.
- zentyal-ftp: configura un server FTP con autenticazione basata su LDAP.
- zentyal-ids: integra un sistema di rilevamento intrusioni nella rete.
- zentyal-ipsec: consente di configurare tunnel IPsec usando OpenSwan.
- zentyal-jabber: integra un server di messaggistica istantanea (XMPP) ejabberd con utenti e gruppi LDAP.
- zentyal-thinclients: soluzione per «thin client» basata su LTSP.
- zentyal-mail: stack completo per la posta che include Postfix e Dovecot con backend LDAP.
- zentyal-mailfilter: configura amavisd con lo stack per filtrare posta indesiderata e virus allegati.
- zentyal-monitor: integra collectd per monitorare le prestazioni del server e i servizi in esecuzione.
- zentyal-pptp: configura un server VPN PPTP.
- zentyal-radius: integra FreeRADIUS con utenti e gruppi LDAP.
- zentyal-software: semplice interfaccia per gestire i moduli installati di Zentyal e gli aggiornamenti del sistema.
- zentyal-trafficshaping: configura le regole del traffico per limitare la larghezza di banda e migliorare la latenza.
- zentyal-usercorner: consente agli utenti di modificare i propri attributi LDAP usando un browser web.
- zentyal-virt: semplice interfaccia per creare e gestire macchine virtuali basate su libvirt.
- zentyal-webmail: consente di accedere alla propria posta usando il popolare servizio di webmail Roundcube.
- zentyal-webserver: configura il server web Apache per ospitare diversi siti sulla propria macchina.
- zentyal-zarafa: integra la suite di software condiviso Zarafa con lo stack per posta elettronica Zentyal e LDAP.

3.2. Primi passi

A ciascun account di sistema appartenente al gruppo «sudo» è consentito l'accesso all'interfaccia web Zentyal. Se si usa l'utente creato durante l'installazione, questo appartiene al gruppo «sudo» per impostazione predefinita.

Se è necessario aggiungere un altro utente al gruppo «sudo», basta eseguire:

```
sudo adduser NOME_UTENTE sudo
```

Per accedere all'interfaccia web Zentyal, navigare in https://localhost/ (o l'IP del proprio server remoto). Zentyal crea e firma il proprio certificato SSL, pertanto è necessario accettare un'eccezione di sicurezza sul proprio browser.

Una volta eseguito l'accesso, verrà visualizzato un cruscotto con una panoramica del server: per configurare le caratteristiche dei moduli installati, aprire le diverse sezioni del menù sulla sinistra. Quando vengono effettuate modifiche, nell'angolo superiore destro appare il pulsante rosso *Save changes* su cui fare clic per salvare tutte le modifiche alla configurazione. Per applicare queste modifiche nel server, è necessario abilitare il modulo, mediante la voce *Module Status* nel menù sulla sinistra. Ogni volta che si abilita un modulo, appare una finestra di popup di conferma prima che vengano eseguite le necessarie operazioni e i cambiamenti sul server e sui file di configurazione.

Per personalizzare il file di configurazione o eseguire determinate azioni (script o comandi) per configurare caratteristiche non disponibili su Zentyal, collocare i modelli dei file di configurazione personalizzata in /etc/zentyal/stubs/<module>/ e i puntatori in /etc/zentyal/hooks/<module>.<action>.

3.3. Riferimenti

Pagina della documentazione ufficiale di *Zentyal*[10].

Consultare anche la pagina della *documentazione della comunità di Zentyal*[11].

Non dimenticare di visitare il *forum*[12] per il supporto della comunità, commenti, richieste di caratteristiche, ecc.

[10] http://doc.zentyal.org/
[11] http://trac.zentyal.org/wiki/Documentation
[12] http://forum.zentyal.org/

Capitolo 7. Autenticazione di rete

Questa sezione applica LDAP all'autenticazione e autorizzazione di rete.

1. Server OpenLDAP

Lightweight Directory Access Protocol (LDAP) è un protocollo per interrogare e modificare un servizio di directory basato su X.500 funzionante su TCP/IP. La versione attuale di LDAP è LDAPv3, come definita in *RFC4510*[1] e l'implementazione di LDAP usata in Ubuntu è OpenLDAP, attualmente alla versione 2.4.25 (Oneiric).

Questo protocollo accede alle directory LDAP; ecco alcuni concetti e termini basilari:

- Una directory LDAP è un albero di *voci* organizzato gerarchicamente, chiamato Directory Information Tree (DIT).
- Una voce consiste in un insieme di *attributi*.
- Un attributo ha un *tipo* (un nome o una descrizione) e uno o più *valori*.
- Ogni attributo deve essere definito in almeno una *classe oggetto (objectClass)*.
- Attributi e classi oggetto sono definiti in *schemi* (una classe oggetto è in definitiva considerata come uno speciale tipo di attributo).
- Ogni voce ha un identificativo unico: è il *Nome distinto (Distinguished Name - DN o dn)*, che consiste del *Nome distinto relativo (Relative Distinguished Name - RDN)* seguito dal DN della voce superiore.
- Il DN della voce non è un attributo e non è considerato parte della voce stessa.

I termini *oggetto*, *contenitore* e *nodo* hanno determinate connotazioni, ma essenzialmente indicano tutti la medesima cosa di *voce*, il termine tecnicamente corretto.

Per esempio, di seguito viene mostrata una singola voce composta da 11 attributi: il suo DN è "cn=John Doe,dc=example,dc=com"; il suo RDN è "cn=John Doe"; e il suo DN superiore è "dc=example,dc=com".

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Larry Smith,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

La voce precedente è in formato *LDIF* (LDAP Data Interchange Format - Formato di interscambio di dati LDAP). Ogni informazione da inserire nel DIT deve essere in tale formato, definito in *RFC2849*[2].

---

[1] http://tools.ietf.org/html/rfc4510
[2] http://tools.ietf.org/html/rfc2849

Sebbene questa guida descriva il suo utilizzo per l'autenticazione centrale, LDAP è ottimo per qualunque attività che necessiti di richieste di accesso a un backend basato su attributi (nome:valore) principalmente in lettura, per esempio una rubrica di indirizzi, un elenco di indirizzi di posta elettronica e una configurazione di un server mail.

1.1. Installazione

Installare il demone server OpenLDAP e le tradizionali utilità di gestione di LDAP che si trovano rispettivamente nei pacchetti slapd e ldap-utils.

L'installazione di sldap crea una configurazione funzionante; in particolare crea un'istanza di database da usare per memorizzare i dati. Tuttavia il suffisso (o il DN base) di questa istanza sono determinati dal nome del dominio dell'host locale. Se necessario, è possibile modificare `/etc/hosts` sostituendo il nome del dominio con uno che fornisce un suffisso diverso. Per esempio, se è necessario un suffisso di *dc=example,dc=com*, il file deve contenere una riga simile alla seguente:

```
127.0.1.1 hostname.example.com hostname
```

È possibile annullare la modifica dopo l'installazione del pacchetto.

Questa guida utilizzerà come suffisso del database *dc=example,dc=com*.

Proseguire con l'installazione:

```
sudo apt-get install slapd ldap-utils
```

Fin da Ubuntu 8.10 slapd è progettato per essere configurato all'interno dello stesso slapd, dedicando un DIT separato per tale scopo; questo consente di configurare dinamicamente slapd senza necessità di riavviare il servizio. Questo database di configurazione consiste in un insieme di file LDIF testuali localizzati in `/etc/ldap/slapd.d`. Questa metodologia è chiamata in diversi modi: metodo slapd-config, metodo RTC (Real Time Configuration - configurazione in tempo reale) o metodo cn=config. È comunque possibile utilizzare il metodo tradizionale con un semplice file, ma ciò è sconsigliato; la funzionalità sarà in futuro gradualmente eliminata.

Ubuntu utilizza il metodo *slapd-config* per la configurazione di slapd e questa guida rispecchia questa scelta.

Durante l'installazione viene richiesto di definire le credenziali di amministratore: si tratta di credenziali LDAP per il *rootDN* dell'istanza di database. Per impostazione predefinita, il DN dell'utente è *cn=admin,dc=example,dc=com* e non viene creato nessun account amministratore per il database slapd-config: è pertanto necessario autenticarsi esternamente a LDAP per poter accedere al database; questo procedimento verrà illustrato in seguito.

Alcuni schemi classici (cosine, nis, inetorgperson) sono attualmente integrati in slapd; è incluso anche uno schema «principale» (core), un pre-requisito per il funzionamento di qualsiasi schema.

1.2. Ispezione post-installazione

Il processo d'installazione imposta 2 DIT: uno per slapd-config e uno per i dati (dc=example,dc=com).

- Questo è l'aspetto del database/DIT di slapd-config: si ricorda che questo database è del tipo LDIF ed è collocato in `/etc/ldap/slapd.d`:

```
   /etc/ldap/slapd.d/

### cn=config
# ### cn=module{0}.ldif
# ### cn=schema
# # ### cn={0}core.ldif
# # ### cn={1}cosine.ldif
# # ### cn={2}nis.ldif
# # ### cn={3}inetorgperson.ldif
# ### cn=schema.ldif
# ### olcBackend={0}hdb.ldif
# ### olcDatabase={0}config.ldif
# ### olcDatabase={-1}frontend.ldif
# ### olcDatabase={1}hdb.ldif
### cn=config.ldif
```

Non modificare direttamente il database slapd-config, ma effettuare le modifiche attraverso il protocollo LDAP (utilità).

- Questo è l'aspetto del DIT di slapd-config tramite il protocollo LDAP:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn

dn: cn=config

dn: cn=module{0},cn=config

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: olcBackend={0}hdb,cn=config

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config
```

```
dn: olcDatabase={1}hdb,cn=config
```

Spiegazione delle voci:

- *cn=config*: impostazioni globali
- *cn=module{0},cn=config*: un modulo caricato dinamicamente
- *cn=schema,cn=config*: contiene uno schema a codifica fissa a livello di sistema
- *cn={0}core,cn=schema,cn=config*: lo schema principale (core) a codifica fissa
- *cn={1}cosine,cn=schema,cn=config*: lo schema cosine
- *cn={2}nis,cn=schema,cn=config*: lo schema nis
- *cn={3}inetorgperson,cn=schema,cn=config*: lo schema inetorgperson
- *olcBackend={0}hdb,cn=config*: il backend di memorizzazione tipo «hdb»
- *olcDatabase={-1}frontend,cn=config*: database frontend, impostazioni predefinite per altri database
- *olcDatabase={0}config,cn=config*: database di configurazione di slapd (cn=config)
- *olcDatabase={1}hdb,cn=config*: l'istanza del proprio database (dc=example,dc=com)

- Questo è l'aspetto del DIT dc=example,dc=com:

```
ldapsearch -x -LLL -H ldap:/// -b dc=example,dc=com dn

dn: dc=example,dc=com

dn: cn=admin,dc=example,dc=com
```

Spiegazione delle voci:

- *dc=example,dc=com*: base del DIT
- *cn=admin,dc=example,dc=com*: amministratore (rootDN) di questo DIT (impostato durante l'installazione del pacchetto)

1.3. Modificare e popolare il database

Introdurre contenuti nel database; verrà aggiunto quanto segue:

- un nodo chiamato *People* (per memorizzare utenti)
- un nodo chiamato *Groups* (per memorizzare gruppi)
- un gruppo chiamato *miners*
- un utente chiamato *john*

Creare il seguente file LDIF e chiamarlo `add_content.ldif`:

```
dn: ou=People,dc=example,dc=com
```

```
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=example,dc=com
objectClass: organizationalUnit
ou: Groups

dn: cn=miners,ou=Groups,dc=example,dc=com
objectClass: posixGroup
cn: miners
gidNumber: 5000

dn: uid=john,ou=People,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 10000
gidNumber: 5000
userPassword: johnldap
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
```

È importante che i valori per uid e gid nella directory non siano in conflitto con i valori locali. Usare intervalli di numeri elevati, per esempio iniziando da 5000; l'impostazione in ldap di valori elevati per uid e gid rende più semplice il controllo di cosa si può fare con un utente locale rispetto a un utente ldap, come verrà meglio indicato in seguito.

Aggiungere il contenuto:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f add_content.ldif
```

```
Enter LDAP Password: ********
adding new entry "ou=People,dc=example,dc=com"

adding new entry "ou=Groups,dc=example,dc=com"

adding new entry "cn=miners,ou=Groups,dc=example,dc=com"

adding new entry "uid=john,ou=People,dc=example,dc=com"
```

È possibile controllare che le informazioni siano state aggiunte correttamente con l'utilità ldapsearch:

```
ldapsearch -x -LLL -b dc=example,dc=com 'uid=john' cn gidNumber
```

```
dn: uid=john,ou=People,dc=example,dc=com
cn: John Doe
gidNumber: 5000
```

Spiegazione delle opzioni:

- *-x:*: autenticazione «semplice»; non usa il metodo predefinito SASL
- *-LLL:*: disabilita la stampa delle informazioni non pertinenti
- *uid=john:*: un «filtro» per cercare l'utente «john»
- *cn gidNumber:*: richiede la visualizzazione di determinati attributi (per impostazione predefinita vengono visualizzati tutti gli attributi)

1.4. Modificare il database di configurazione di slapd

Il DIT di slapd-config può anche essre interrogato e modificato: ecco alcuni esempi.

- Usare ldapmodify per aggiungere un «Indice» (attributo DbIndex) al {1}hdb,cn=config del database (dc=example,dc=com). Creare un file chiamato `uid_index.ldif`, con i seguenti contenuti:

  ```
  dn: olcDatabase={1}hdb,cn=config
  add: olcDbIndex
  olcDbIndex: uid eq,pres,sub
  ```

  Quindi eseguire il comando:

  ```
  sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f uid_index.ldif

  modifying entry "olcDatabase={1}hdb,cn=config"
  ```

  È possibile confermare la modifica digitando:

  ```
  sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=config '(olcDatabase={1}hdb)' olcDbIndex

  dn: olcDatabase={1}hdb,cn=config
  olcDbIndex: objectClass eq
  olcDbIndex: uid eq,pres,sub
  ```

- Aggiungere uno schema: è necessario convertirlo nel formato LDIF. È possibile trovare sia schemi non convertiti che convertiti nella directory `/etc/ldap/schema`.

- Rimuovere uno schema dal database slapd-config non è un'operazione di poco conto: esercitarsi ad aggiungere schemi su un sistema di prova.
- Prima di aggiungere uno schema, è necessario controllare quali schemi sono stati già installati (quello visualizzato è un output predefinito, pronto per l'uso)

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=schema,cn=config dn

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config
```

Nel seguente esempio, verrà aggiunto lo schema CORBA.

1. Creare il file di configurazione della conversione `schema_convert.conf` contenente le seguenti righe:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/ldapns.schema
include /etc/ldap/schema/pmi.schema
```

2. Creare la directory di output `ldif_output`.
3. Determinare l'indice dello schema:

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | grep corba,cn=schema

cn={1}corba,cn=schema,cn=config
```

Quando slapd inserisce oggetti con lo stesso DN superiore, crea un *indice* per quell'oggetto; l'indice viene racchiuso fra parentesi graffe: {X}.

4. Usare slapcat per effettuare la conversione:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \ ldap:///cn={1}corba,cn=schema,cn=confi
```

Lo schema convertito è ora in `cn=corba.ldif`

5. Modificare `cn=corba.ldif` per giungere ai seguenti attributi:

```
dn: cn=corba,cn=schema,cn=config
...
cn: corba
```

Rimuovere anche le seguenti righe dal fondo:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 52109a02-66ab-1030-8be2-bbf166230478
creatorsName: cn=config
createTimestamp: 20110829165435Z
entryCSN: 20110829165435.935248Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20110829165435Z
```

I valori degli attributi variano.

6. Infine, usare ldapadd per aggiungere il nuovo schema al DIT di slapd-config:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=corba.ldif

adding new entry "cn=corba,cn=schema,cn=config"
```

7. Confermare gli schemi attualmente caricati:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config dn

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: cn={4}corba,cn=schema,cn=config
```

Affinché le applicazioni esterne e i client possano autenticarsi usando LDAP, è necessario che siano configurati a tal fine; consultare la documentazione relativa ai client per ulteriori dettagli.

1.5. Registrazione

L'attività di registrazione in slapd è indispensabile per l'implementazione di una soluzione basata su OpenLDAP, ma deve essere abilitata manualmente dopo l'installazione del software, altrimenti

nei registri sarebbero visualizzati solo dei messaggi rudimentali. La registrazione, come ogni altra configurazione slapd, è abilitata tramite database slapd-config.

OpenLDAP è dotato di sottosistemi di registrazione multipli (livelli) ognuno dei quali contiene quello di livello inferiore (additivo); un buon livello da provare è *stats*. La pagina del manuale di *slapd-config*[3] contiene maggiori particolari sui diversi sottosistemi.

Creare il file `logging.ldif` con i seguenti contenuti:

```
dn: cn=config
changetype: modify
add: olcLogLevel
olcLogLevel: stats
```

Implementare la modifica:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f logging.ldif
```

Questo produce un significativo ammontare di registrazioni, che potrebbe essere necessario ridure a un livello di dettaglio inferiore quando il sistema è in produzione. Mentre è in questa modalità dettagliata, la macchina syslog dell'host (rsyslog) potrebbe incontrare difficoltà nel tenere il passo, fornendo messaggi simili al seguente:

```
rsyslogd-2177: imuxsock lost 228 messages from pid 2547 due to rate-limiting
```

Può essere necessaria una modifica della configurazione di rsyslog: in `/etc/rsyslog.conf`, inserire:

```
# Disable rate limiting
# (default is 200 messages in 5 seconds; below we make the 5 become 0)
$SystemLogRateLimitInterval 0
```

E riavviare il demone rsyslog:

```
sudo service rsyslog restart
```

1.6. Replicazione

Il servizio LDAP diventa sempre più importante quando più sistemi in rete iniziano a dipendere da esso. In questa situazione, viene normalmente predisposto in LDAP un sistema di ridondanza (alta disponibilità), allo scopo di prevenire serie problematiche conseguenti alla mancata risposta da parte del server LDAP; questo obiettivo viene raggiunto per mezzo della *replicazione*.

La replicazione è ottenuta utilizzando il motore *Syncrepl*; questo consente alle modifiche di essere sincronizzate usando un modello *consumatore* - *fornitore*. Il tipo specifico di replicazione che verrà implementato in questa guida è una combinazione delle seguenti modalità: *refreshAndPersist* e

[3] http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html

delta-syncrepl. Il fornitore invia le voci modificate al consumatore non appena vengono effettuate le modifiche ma vengono inviate solamente le modifiche, non le intere voci.

1.6.1. Configurazione del fornitore

Iniziare configurando il *fornitore*.

1. Creare un file LDIF chiamato `provider_sync.ldif` con i seguenti contenuti:

```
# Add indexes to the frontend db.
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

#Load the syncprov and accesslog modules.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov
-
add: olcModuleLoad
olcModuleLoad: accesslog

# Accesslog database definitions
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap/accesslog
olcSuffix: cn=accesslog
olcRootDN: cn=admin,dc=example,dc=com
olcDbIndex: default eq
olcDbIndex: entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog db syncprov.
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE

# syncrepl Provider for primary db
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
```

```
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

# accesslog overlay definitions for primary db
dn: olcOverlay=accesslog,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcAccessLogConfig
olcOverlay: accesslog
olcAccessLogDB: cn=accesslog
olcAccessLogOps: writes
olcAccessLogSuccess: TRUE
# scan the accesslog DB every day, and purge entries older than 7 days
olcAccessLogPurge: 07+00:00 01+00:00
```

Modificare il rootDN nel file LDIF per farlo coincidere con quello presente nella propria directory.

2. Il profilo per slapd apparmor deve essere adattato in relazione alla posizione del database accesslog; modificare `/etc/apparmor.d/local/usr.sbin.slapd` aggiungendo quanto segue:

```
/var/lib/ldap/accesslog/ r,
/var/lib/ldap/accesslog/** rwk,
```

Creare una directory, impostare un file di configurazione del database e ricaricare il profilo apparmor:

```
sudo -u openldap mkdir /var/lib/ldap/accesslog
sudo -u openldap cp /var/lib/ldap/DB_CONFIG /var/lib/ldap/accesslog
sudo service apparmor reload
```

3. Aggiungere i nuovi contenuti e, considerato che apparmor è stato modificato, riavviare il demone:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f provider_sync.ldif
sudo service slapd restart
```

Il fornitore è ora configurato.

1.6.2. Configurazione del «consumatore»

Configurare ora il *«consumatore»*.

1. Installare il software tramite *Sezione 1.1, «Installazione» [94]*; assicurarsi che il database slapd-config sia identico a quello del fornitore: in particolare, assicurarsi che gli schemi e il suffisso del database siano gli stessi.
2. Creare un file LDIF chiamato `consumer_sync.ldif` con i seguenti contenuti:

```
dn: cn=module{0},cn=config
```

```
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov

dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com bindmethod=simple binddn="cn=admin,dc=exa
 credentials=secret searchbase="dc=example,dc=com" logbase="cn=accesslog"
 logfilter="(&(objectClass=auditWriteObject)(reqResult=0))" schemachecking=on
 type=refreshAndPersist retry="60 +" syncdata=accesslog
-
add: olcUpdateRef
olcUpdateRef: ldap://ldap01.example.com
```

Assicurarsi che i seguenti attributi abbiano i valori corretti:

- *provider* (nome host del server del fornitore -- ldap01.example.com in questo esempio -- o indirizzo IP)
- *binddn* (il DN dell'amministratore in uso)
- *credentials* (la password del DN dell'amministratore in uso)
- *searchbase* (il suffisso del database in uso)
- *olcUpdateRef* (nome host del server del fornitore o indirizzo IP)
- *rid* (Replica ID, un numero di tre cifre univoco che identifica la replica: ogni «consumatore» dovrebbe avere almeno un rid)

3. Aggiungere i nuovi contenuti:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f consumer_sync.ldif
```

Fatto, i due database (suffix: dc=example,dc=com) dovrebbero sincronizzarsi.

1.6.3. Test

Una volta iniziata la replicazione, è possibile controllare il processo eseguendo:

```
ldapsearch -z1 -LLLQY EXTERNAL -H ldapi:/// -s base contextCSN

dn: dc=example,dc=com
contextCSN: 20120201193408.178454Z#000000#000#000000
```

sia sul fornitore che sul consumatore. Quando l'output (`20120201193408.178454Z#000000#000#000000` nel precedente esempio) su entrambe le macchine corrisponde, si è ottenuta la replicazione. Ogni volta che viene effettuata una modifica sul fornitore, questo valore cambierà e lo stesso dovrebbe accadere a quello dei consumatori.

Se la connessione è lenta o il database ldap grande, potrebbe occorrere del tempo prima che il *contextCSN* del consumatore corrisponda a quello del fornitore, ma sarà possibile controllare che il processo è ancora in corso, dal momento che il *contextCSN* del consumatore crescerà costantemente.

Se il *contextCSN* del consumatore manca o non corrisponde a quello del fornitore, è necessario fermarsi e risolvere il problema, prima di continuare. Provare a controllare i file di registro di slapd (syslog) e di auth nel fornitore per controllare che la richiesta di autenticazione del consumatore abbia avuto successo o che le sue richieste di recupero di dati (che somigliano a istruzioni di ldapsearch) non restituiscano errori.

Per verificare che il processo sia andato a buon fine, basta cercare, sul «consumatore», i DN nel database:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b dc=example,dc=com dn
```

Dovrebbero essere visualizzati l'utente «john», il gruppo «miners» e i nodi «People» e «Groups».

1.7. Controllo degli accessi

La gestione del tipo di accesso alle risorse (lettura, scrittura, ecc.) da accordare agli utenti è conosciuta come *controllo degli accessi*. Le direttive di configurazione richieste sono chiamate *elenchi di controllo degli accessi* (access control lists) o ACL.

Durante l'installazione del pacchetto slapd vengono impostate automaticamente diversi ACL. Verranno esaminate alcune importanti conseguenze di queste impostazioni predefinite, in modo da dare un'idea del funzionamento e della configurazione degli ACL.

Per ottenere ACL efficaci per una interrogazione LDAP è necessario esaminare sia le voci ACL del database che viene interrogato che quelle della speciale istanza del database del frontend. Gli ACL di quest'ultimo operano come predefiniti in caso quelli del primo non corrispondano. Il database del frontend viene interrogato per secondo e vengono applicati i primi ACL che trovano corrispondenza («la prima corrispondenza vince») fra queste due fonti di ACL. I seguenti comandi restituiscono, rispettivamente, gli ACL del database hdb («"dc=example,dc=com"x) e quelli del database del frontend:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=config '(olcDatabase={1}hdb)' olcAccess

dn: olcDatabase={1}hdb,cn=config
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymous
              auth by dn="cn=admin,dc=example,dc=com" write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by self write by dn="cn=admin,dc=example,dc=com" write by *
  read
```

Il rootDN gode sempre di pieni diritti d'accesso al suo database; includerlo in un ACL non fornisce un'esplicita configurazione ma provoca un calo di prestazioni in slapd.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=config '(olcDatabase={-1}frontend)' olcAcc
```

```
dn: olcDatabase={-1}frontend,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
             cn=external,cn=auth manage by * break
olcAccess: {1}to dn.exact="" by * read
olcAccess: {2}to dn.base="cn=Subschema" by * read
```

Il primo ACL è cruciale:

```
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymous
              auth by dn="cn=admin,dc=example,dc=com" write by * none
```

Questo può essere diversamente rappresentato per una più semplice comprensione:

```
to attrs=userPassword
 by self write
 by anonymous auth
 by dn="cn=admin,dc=example,dc=com" write
 by * none

to attrs=shadowLastChange
 by self write
 by anonymous auth
 by dn="cn=admin,dc=example,dc=com" write
 by * none
```

Questo ACL composto (ce ne sono 2) impone quanto segue:

- L'accesso anonimo «auth» è fornito all'attributo *userPassword* per la connessione iniziale. In maniera forse poco intuitiva, «by anonymous auth» è necessario anche quando non sia richiesto un accesso anonimo al DIT. Una volta che l'interfaccia remota è collegata, tuttavia, l'autenticazione può essere effettuata (vedere il prossimo punto).
- L'autenticazione può avvenire in quanto tutti gli utenti hanno accesso «in lettura» (fornito dall'istruzione «by self write») all'attributo *userPassword*.
- L'attributo *userPassword* non è altrimenti accessibile da tutti gli altri utenti, con l'eccezione del rootDN, che ne ha un accesso completo.
- Per consentire agli utenti la modifica della propria password, usando il comando **passwd** o altre utilità, è necessario che l'attributo *shadowLastChange* sia accessibile dopo l'autenticazione dell'utente.

Questo DIT può essere esaminato in maniera anonima in quanto è presente l'istruzione «by * read» in questo ACL:

```
to *
 by self write
```

```
 by dn="cn=admin,dc=example,dc=com" write
 by * read
```

Se ciò non è richiesto, è necessario modificare l'ACL. Per forzare l'autenticazione durante una richiesta di collegamento, è possibile in alternativa (o in combinazione con la modifica dell'ACL) usare l'istruzione «olcRequire: authc».

Come menzionato in precedenza, nel database slapd-config non viene creato nessun account amministratore. Esiste tuttavia la seguente identità SASL alla quale è garantito pieno accesso, che rappresenta il superutente dell'host locale (root/sudo):

```
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

Il seguente comando visualizza gli ACL del database slapd-config:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=config '(olcDatabase={0}config)' olcAccess

dn: olcDatabase={0}config,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
              cn=external,cn=auth manage by * break
```

Dal momento che questa è un'identità SASL, è necessario usare un *meccanismo* SASL nel momento in cui si invoca l'utilità LDAP in questione, come più volte illustrato in questa guida: si tratta del meccanismo EXTERNAL. Esaminare come esempio il precedente comando. Si noti che:

1. È necessario usare *sudo* per assumere l'identità root e trovare corrispondenza con l'ACL.
2. Il meccanismo EXTERNAL funziona tramite *IPC* (socket del dominio UNIX): ciò significa che è necessario usare il formato URI *ldapi*

Un modo sintetico per ottenere tutti gli ACL è simile al seguente:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=config '(olcAccess=*)' olcAccess olcSuffix
```

Maggiori particolari sull'argomento del controllo degli accessi possono essere rinvenuti nella pagina del manuale *slapd.access*[4].

1.8. TLS

Nell'autenticarsi a un server OpenLDAP è meglio usare una sessione cifrata: questo risultato può essere raggiunto usando Transport Layer Security (TLS).

In questo caso, assumendo di essere la propria *Autorità di Certificazione*, creare e firmare il proprio certificato server LDAP. Dal momento che slapd è compilato usando la libreria gnutls, è necessario usare l'utilità certtool per completare questi processi.

[4] http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html

1. Installare i pacchetti gnutls-bin e ssl-cert:

```
sudo apt-get install gnutls-bin ssl-cert
```

2. Creare una chiave privata per l'Autorità di Certificazione:

```
sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"
```

3. Creare il file o il modello `/etc/ssl/ca.info` per definire la CA:

```
cn = Example Company
ca
cert_signing_key
```

4. Creare il certificato CA auto-firmato:

```
sudo certtool --generate-self-signed \ --load-privkey /etc/ssl/private/cakey.pem \ --template /
```

5. Creare una chiave primaria per il server:

```
sudo certtool --generate-privkey \ --bits 1024 \ --outfile /etc/ssl/private/ldap01_slapd_key.pe
```

Sostituire *ldap01* nel nome del file con il nome host del proprio server. Per mantenere un certo ordine, sarebbe opportuno chiamare il certificato e la chiave come l'host e il servizio per cui saranno usati.

6. Creare il file info `/etc/ssl/ldap01.info` contenente:

```
organization = Società Esempio
cn = ldap01.example.com
tls_www_server
chiave_cifratura
chiave_firma
expiration_days = 3650
```

Il precedente certificato è valido per 10 anni: modificarlo in base al proprio caso.

7. Creare il certificato del server:

```
sudo certtool --generate-certificate \ --load-privkey /etc/ssl/private/ldap01_slapd_key.pem \ -
```

Creare il file `certinfo.ldif` con i seguenti contenuti (nell'esempio si assume che siano stati creati certificati usando https://www.cacert.org, modificare il file in base al proprio caso):

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
```

```
olcTLSCertificateFile: /etc/ssl/certs/ldap01_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap01_slapd_key.pem
```

Usare il comando ldapmodify per comunicare a slapd le impostazioni TLS effettuate tramite il database slapd-config:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/ssl/certinfo.ldif
```

Contrariamente a quanto si crede comunemente, non è necessario usare *ldaps://* in `/etc/default/slapd` per ottenere la cifratura, basta avere:

```
SLAPD_SERVICES="ldap:/// ldapi:///"
```

LDAP su TLS/SSL (ldaps://) è sconsigliato in favore di *StartTLS*. Quest'ultimo fa riferimento a una sessione LDAP esistente (in ascolto con protocollo TCP sulla porta 389) che viene successivamente protetto da TLS/SSL mentre LDAPS, come HTTPS, è un distinto protocollo, cifrato fin dall'inizio, che opera sulla porta TCP 636.

Rafforzare la proprietà e i permessi:

```
sudo adduser openldap ssl-cert
sudo chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap01_slapd_key.pem
```

Riavviare OpenLDAP:

```
sudo service slapd restart
```

Controllare i log dell'host (/var/log/syslog) per verificare che il server si sia avviato correttamente.

1.9. Replicazione e TLS

Se è stata impostata la replicazione tra server, è procedura comune cifrare (StartTLS) il traffico di replicazione per prevenire intercettazioni: ciò è diverso dall'utilizzo della cifratura con l'autenticazione trattato in precedenza. In questa sezione verrà sviluppato il funzionamento dell'autenticazione TLS.

Si assume che sia stata impostata la replicazione tra il fornitore e il consumatore come descritto in *Sezione 1.6, «Replicazione» [101]* e TLS sia stato configurato per l'autenticazione sul fornitore come spiegato in *Sezione 1.8, «TLS» [107]*.

Come spiegato in precedenza, l'obiettivo della replicazione è aumentare la disponibilità del servizio LDAP. Avendo impostato l'autenticazione di TLS sul fornitore, si richiede la stessa cosa sul

consumatore; oltre a questo, è necessario cifrare il traffico di replicazione. Rimane da creare una chiave e un certificato per il consumatore e quindi effettuare una configurazione secondo le proprie esigenze. La chiave e il certificato verranno generati sul fornitore, per evitare di creare un altro certificato CA, e il materiale necessario verrà quindi trasferito sul consumatore.

1. Sul fornitore,

   Creare una directory principale (che verrà usata per gli eventuali trasferimenti) e quindi la chiave privata del «Consumatore»:

   ```
   mkdir ldap02-ssl
   cd ldap02-ssl
   sudo certtool --generate-privkey \ --bits 1024 \ --outfile ldap02_slapd_key.pem
   ```

   Creare un file info, `ldap02.info`, per il server «Consumatore», adattando i suoi valori in base alle proprie esigenze:

   ```
   organization = Società Esempio
   cn = ldap02.example.com
   tls_www_server
   chiave_cifratura
   chiave_firma
   expiration_days = 3650
   ```

   Creare il certificato del «Consumatore»:

   ```
   sudo certtool --generate-certificate \ --load-privkey ldap02_slapd_key.pem \ --load-ca-certific
   ```

   Ottenere una copia del certificato CA:

   ```
   cp /etc/ssl/certs/cacert.pem .
   ```

   Fatto. Ora trasferire la directory `ldap02-ssl` al «Consumatore»: in questo caso viene usato scp (modificarlo in base al proprio caso):

   ```
   cd ..
   scp -r ldap02-ssl utente@consumer:
   ```

2. Sul «Consumatore»,

   Configurare l'autenticazione TLS:

   ```
   sudo apt-get install ssl-cert
   sudo adduser openldap ssl-cert
   sudo cp ldap02_slapd_cert.pem cacert.pem /etc/ssl/certs
   sudo cp ldap02_slapd_key.pem /etc/ssl/private
   sudo chgrp ssl-cert /etc/ssl/private/ldap02_slapd_key.pem
   ```

```
sudo chmod g+r /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap02_slapd_key.pem
```

Creare il file `/etc/ssl/certinfo.ldif` con i seguenti contenuti (modificarlo in base al proprio caso):

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap02_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap02_slapd_key.pem
```

Configurare il database slapd-config:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f certinfo.ldif
```

Configurare `/etc/default/slapd` come sul fornitore (SLAPD_SERVICES).

3. Sul «Consumatore»,

   Configurare TLS per la replicazione lato «Consumatore»; modificare l'attributo esistente *olcSyncrepl* aggiungendo alcune opzioni TLS. Nel fare ciò, per la prima volta, si esaminerà la modifica del valore di uno o più attributi.

   Creare il file `consumer_sync_tls.ldif` con i seguenti contenuti:

```
dn: olcDatabase={1}hdb,cn=config
replace: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com bindmethod=simple
 binddn="cn=admin,dc=example,dc=com" credentials=secret searchbase="dc=example,dc=com"
 logbase="cn=accesslog" logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
 schemachecking=on type=refreshAndPersist retry="60 +" syncdata=accesslog
 starttls=critical tls_reqcert=demand
```

   Le opzioni supplementari specificano, rispettivamente, che il consumatore deve usare StartTLS e che per verificare l'identità del fornitore è necessario il certificato CA; notare anche la sintassi di LDIF per la modifica del valore di un attributo («replace»)

   Rendere effettive queste modifiche:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f consumer_sync_tls.ldif
```

   E riavviare slapd:

```
sudo service slapd restart
```

4. Sul fornitore,

   Controllare che sia stata stabilita una sessione TLS: in `/var/log/syslog`, a patto che sia stato impostato un accesso a livello «conns», dovrebbero essere visualizzati messaggi simili ai seguenti:

```
slapd[3620]: conn=1047 fd=20 ACCEPT from IP=10.153.107.229:57922 (IP=0.0.0.0:389)
slapd[3620]: conn=1047 op=0 EXT oid=1.3.6.1.4.1.1466.20037
slapd[3620]: conn=1047 op=0 STARTTLS
slapd[3620]: conn=1047 op=0 RESULT oid= err=0 text=
slapd[3620]: conn=1047 fd=20 TLS established tls_ssf=128 ssf=128
slapd[3620]: conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" method=128
slapd[3620]: conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" mech=SIMPLE ssf=0
slapd[3620]: conn=1047 op=1 RESULT tag=97 err=0 text
```

1.10. Autenticazione LDAP

Una volta ottenuto un server LDAP funzionante, occorre installare sul client le librerie necessarie per sapere come e quando contattarlo. In Ubuntu, questo risultato viene tradizionalmente raggiunto con l'installazione del pacchetto libnss-ldap, che comprende altri strumenti utili nel processo di configurazione. Istallare questo pacchetto:

```
sudo apt-get install libnss-ldap
```

Vengono richiesti dettagli relativi al server LDAP; in caso di errori, è possibile provare di nuovo digitando.

```
sudo dpkg-reconfigure ldap-auth-config
```

I risultati della configurazione possono essere visualizzati nel file `/etc/ldap.conf`. Se il server richiede delle opzioni non contemplate durante la fase di configurazione. modificare il file secondo le proprie esigenze.

Ora configurare il profilo LDAP per NSS:

```
sudo auth-client-config -t nss -p lac_ldap
```

Configurare il sistema per usare LDAP per l'autenticazione:

```
sudo pam-auth-update
```

Dal menù, scegliere LDAP e ogni altro metodo di autenticazione necessario.

Ora dovrebbe essere possibile eseguire l'accesso utilizzando le credenziali LDAP.

I client LDAP devono potersi riferire a diversi server, se viene usata la replicazione; in `/etc/ldap.conf` si dovrebbe avere qualcosa di simile:

```
uri ldap://ldap01.example.com ldap://ldap02.example.com
```

La richiesta scade e il consumatore (ldap02) tenterà di essere raggiunto se il fornitore (ldap01) non risponde.

Se LDAP viene utilizzato per archiviare utenti Samba, è necessario configurare il server Samba affinché utilizzi l'autenticazione LDAP. Per maggiori informazioni, consultare la sezione *Sezione 2, «Samba e LDAP» [119]*.

Un'alternativa al pacchetto libnss-ldap è libnss-ldapd che, tuttavia, comprende il pacchetto nscd, che probabilmente non è necessario: basta rimuoverlo successivamente.

1.11. Gestire utenti e gruppi

Il pacchetto ldap-utils contiene diverse utilità per la gestione di directory, ma le molte opzioni necessarie possono renderle di difficile utilizzo. Il pacchetto ldapscripts contiene degli script «wrapper» per queste utilità che possono semplificare le operazioni.

Installare il pacchetto:

```
sudo apt-get install ldapscripts
```

Quindi modificare il file `/etc/ldapscripts/ldapscripts.conf` per giungere a qualcosa di simile al seguente:

```
SERVER=localhost
BINDDN='cn=admin,dc=example,dc=com'
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX='dc=example,dc=com'
GSUFFIX='ou=Groups'
USUFFIX='ou=People'
MSUFFIX='ou=Computers'
GIDSTART=10000
UIDSTART=10000
MIDSTART=10000
```

Ora creare il file `ldapscripts.passwd` per consentire l'accesso alla directory da parte del rootDN:

```
sudo sh -c "echo -n 'secret' > /etc/ldapscripts/ldapscripts.passwd"
sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd
```

Sostituire ««secret»» con la password dell'utente rootDN.

Gli sript sono ora pronti per la gestione della directory; ecco alcuni esempi sul loro utilizzo:

- Creare un nuovo utente:

```
sudo ldapadduser mario example
```

Viene creato un utente con UID *mario* e imposta il gruppo primario (GID) dell'utente a *example*

- Cambiare la password di un utente:

```
sudo ldapsetpasswd mario
Changing password for user uid=mario,ou=People,dc=example,dc=com
New Password:
New Password (verify):
```

- Eliminare un utente:

```
sudo ldapdeleteuser mario
```

- Aggiungere un gruppo:

```
sudo ldapaddgroup qa
```

- Eliminare un gruppo:

```
sudo ldapdeletegroup qa
```

- Aggiungere un utente a un gruppo:

```
sudo ldapaddusertogroup george qa
```

Dovrebbe essere possibile visualizzare un attributo *memberUid* per il gruppo *qa* con un valore di *mario*.

- Rimuovere un utente da un gruppo:

```
sudo ldapdeleteuserfromgroup george qa
```

L'attributo *memberUid* dovrebbe ora essere rimosso dal gruppo *qa*.

- Lo script ldapmodifyuser consente di aggiungere, rimuovere o replicare gli attributi di un utente. Lo script utilizza la stessa sintassi dell'utilità ldapmodify. Per esempio:

```
sudo ldapmodifyuser george
# About to modify the following entry :
dn: uid=george,ou=People,dc=example,dc=com
objectClass: account
objectClass: posixAccount
cn: george
uid: george
uidNumber: 1001
gidNumber: 1001
```

```
homeDirectory: /home/george
loginShell: /bin/bash
gecos: george
description: User account
userPassword:: e1NTSEF9eXFsTFcyWlhwWkF1eGUybVdFWHZKRzJVMjFTSG9vcHk=

# Enter your modifications here, end with CTRL-D.
dn: uid=george,ou=People,dc=example,dc=com
replace: gecos
gecos: Mario Rossi
```

L'utente *gecos* dovrebbe ora essere «Mario Rossi».

- Un'utile caratteristica di ldapscripts è il sistema dei modelli. I modelli consentono di personalizzare gli attributi di un utente, gruppo e degli oggetti macchina. Per esempio, per abilitare il modello *user*, aprire il file `/etc/ldapscripts/ldapscripts.conf`, modificando:

```
UTEMPLATE="/etc/ldapscripts/ldapadduser.template"
```

Diversi *esempi* sono disponibili nella directory `/etc/ldapscripts`. Copiare o rinominare il file `ldapadduser.template.sample` in `/etc/ldapscripts/ldapadduser.template`:

```
sudo cp /usr/share/doc/ldapscripts/examples/ldapadduser.template.sample \ /etc/ldapscripts/ldapad
```

Modificare il nuovo modello per aggiungere gli attributi desiderati: in questo esempio viene creato un nuovo utente con una objectClass di inetOrgPerson:

```
dn: uid=<user>,<usuffix>,<suffix>
objectClass: inetOrgPerson
objectClass: posixAccount
cn: <user>
sn: <ask>
uid: <user>
uidNumber: <uid>
gidNumber: <gid>
homeDirectory: <home>
loginShell: <shell>
gecos: <user>
description: User account
title: Employee
```

Notare l'opzione *<ask>* utilizzata per l'attributo *sn*, in questo modo ldapadduser chiederà di inserire il suo valore.

Nel pacchetto sono presenti utilità non illustrate in questo documento. Ecco un elenco completo:

`ldaprenamemachine`[5]

[5] http://manpages.ubuntu.com/manpages/en/man1/ldaprenamemachine.1.html

ldapadduser[6]
ldapdeleteuserfromgroup[7]
ldapfinger[8]
ldapid[9]
ldapgid[10]
ldapmodifyuser[11]
ldaprenameuser[12]
lsldap[13]
ldapaddusertogroup[14]
ldapsetpasswd[15]
ldapinit[16]
ldapaddgroup[17]
ldapdeletegroup[18]
ldapmodifygroup[19]
ldapdeletemachine[20]
ldaprenamegroup[21]
ldapaddmachine[22]
ldapmodifymachine[23]
ldapsetprimarygroup[24]
ldapdeleteuser[25]

1.12. Backup e ripristino

Ora che ldap funziona come si deve, è necessario assicurarsi di salvare tutto il lavoro per poterlo ripristinare, in caso di necessità.

È necessario disporre di un modo di effettuare il backup dei database di ldap, in particolare del backend (cn=config) e del frontend (dc=example, dc=com). Per effetture il backup di questi database in un file, per esempio `/export/backup`, è possibile usare slapcat, come mostrato nel seguente script, chiamato `/usr/local/bin/ldapbackup`:

```
#!/bin/bash
```

[6] http://manpages.ubuntu.com/manpages/en/man1/ldapadduser.1.html
[7] http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuserfromgroup.1.html
[8] http://manpages.ubuntu.com/manpages/en/man1/ldapfinger.1.html
[9] http://manpages.ubuntu.com/manpages/en/man1/ldapid.1.html
[10] http://manpages.ubuntu.com/manpages/en/man1/ldapgid.1.html
[11] http://manpages.ubuntu.com/manpages/en/man1/ldapmodifyuser.1.html
[12] http://manpages.ubuntu.com/manpages/en/man1/ldaprenameuser.1.html
[13] http://manpages.ubuntu.com/manpages/en/man1/lsldap.1.html
[14] http://manpages.ubuntu.com/manpages/en/man1/ldapaddusertogroup.1.html
[15] http://manpages.ubuntu.com/manpages/en/man1/ldapsetpasswd.1.html
[16] http://manpages.ubuntu.com/manpages/en/man1/ldapinit.1.html
[17] http://manpages.ubuntu.com/manpages/en/man1/ldapaddgroup.1.html
[18] http://manpages.ubuntu.com/manpages/en/man1/ldapdeletegroup.1.html
[19] http://manpages.ubuntu.com/manpages/en/man1/ldapmodifygroup.1.html
[20] http://manpages.ubuntu.com/manpages/en/man1/ldapdeletemachine.1.html
[21] http://manpages.ubuntu.com/manpages/en/man1/ldaprenamegroup.1.html
[22] http://manpages.ubuntu.com/manpages/en/man1/ldapaddmachine.1.html
[23] http://manpages.ubuntu.com/manpages/en/man1/ldapmodifymachine.1.html
[24] http://manpages.ubuntu.com/manpages/en/man1/ldapsetprimarygroup.1.html
[25] http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuser.1.html

```
BACKUP_PATH=/export/backup
SLAPCAT=/usr/sbin/slapcat

nice ${SLAPCAT} -n 0 > ${BACKUP_PATH}/config.ldif
nice ${SLAPCAT} -n 1 > ${BACKUP_PATH}/example.com.ldif
nice ${SLAPCAT} -n 2 > ${BACKUP_PATH}/access.ldif
chmod 640 ${BACKUP_PATH}/*.ldif
```

Vengono creati dei file di testo non compressi, che contengono tutto ciò che si trova nei database ldap, compreso la disposizione dell'albero, i nomi utente e tutte le password. Occorre pertanto prendere in considerazione l'opportunità di rendere `/export/backup` una partizione cifrata e anche di far sì che lo script proceda a cifrare i file mentre vengono creati. L'ideale sarebbe effettuare entrambe queste operazioni, ma questo dipende dai requisiti di sicurezza richiesti.

Ora, si tratta solo di creare uno script cron per eseguire questo programma con la periodicità ritenuta necessaria; nella maggior parte dei casi è sufficiente una volta al giorno, ma potrebbe essere necessaria una frequenza maggiore. Ecco un esempio di script cron chiamato `/etc/cron.d/ldapbackup` che viene eseguito ogni notte alle ore 22:45:

```
MAILTO=backup-emails@domain.com
45 22 * * * root /usr/local/bin/ldapbackup
```

Ora che i file sono stati creati, è necessario copiarli in un server di backup.

Se ldap è stato reinstallato recentemente, il processo di ripristino dovrebbe essere simile al seguente:

```
sudo service slapd stop
sudo mkdir /var/lib/ldap/accesslog
sudo slapadd -F /etc/ldap/slapd.d -n 0 -l /export/backup/config.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 1 -l /export/backup/domain.com.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 2 -l /export/backup/access.ldif
sudo chown -R openldap:openldap /etc/ldap/slapd.d/
sudo chown -R openldap:openldap /var/lib/ldap/
sudo service slapd start
```

1.13. Risorse

- La principale risorsa nella documentazione upstream: *www.openldap.org*[26]
- Ci sono molte pagine del manuale che trattano il pacchetto slapd: eccone alcune importanti, specialmente considerando il materiale presentato in questa guida:

  slapd[27]

[26] http://www.openldap.org/

[27] http://manpages.ubuntu.com/manpages/en/man8/slapd.8.html

slapd-config[28]
slapd.access[29]
slapo-syncprov[30]

- Altre pagine del manuale:

auth-client-config[31]
pam-auth-update[32]

- Il manuale online di Zytrax *LDAP for Rocket Scientists*[33], un modo di trattare LDAP meno cattedratico ma esauriente
- La pagina della *documentazione della comunità su OpenLDAP*[34] contiene una collezione di note
- *LDAP System Administration*[35] di O'Reilly (libro di testo; 2003)
- *Mastering OpenLDAP*[36] di Packt (libro di testo; 2007)

28 http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html
29 http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html
30 http://manpages.ubuntu.com/manpages/en/man5/slapo-syncprov.5.html
31 http://manpages.ubuntu.com/manpages/en/man8/auth-client-config.8.html
32 http://manpages.ubuntu.com/manpages/en/man8/pam-auth-update.8.html
33 http://www.zytrax.com/books/ldap/
34 https://help.ubuntu.com/community/OpenLDAPServer
35 http://www.oreilly.com/catalog/ldapsa/
36 http://www.packtpub.com/OpenLDAP-Developers-Server-Open-Source-Linux/book

2. Samba e LDAP

Questa sezione illustra l'integrazione di Samba con LDAP. Il ruolo del server Samba è quello di server «autonomo» e la directory LDAP fornisce l'autenticazione, oltre a contenere le informazioni dell'account dell'utente, del gruppo, e della macchina richiesti da Samba per il suo funzionamento (in ognuno dei 3 possibili ruoli). Il prerequisito è un server OpenLDAP configurato con una directory in grado di accettare richieste di autenticazione. Per maggiori dettagli sul modo di soddisfare questo requisito, consultare *Sezione 1, «Server OpenLDAP» [93]*. Terminata la consultazione di questa sezione, si dovrà decidere quali funzionalità specifiche di Samba siano necessarie e configurarlo di conseguenza.

2.1. Installazione del software

Sono necessari tre pacchetti per integrare Samba con LDAP: samba, samba-doc e smbldap-tools.

A rigor di termini, il pacchetto smbldap-tools non è necessario, ma è meglio installarlo, a meno di non disporre di un modo alternativo per gestire le varie entità Samba (utenti, gruppi, computer) in un contesto LDAP.

Installare questi pacchetti:

```
sudo apt-get install samba samba-doc smbldap-tools
```

2.2. Configurazione di LDAP

È necessario configurare il server LDAP affinché possa contenere dati Samba; in questa sezione verranno eseguiti tre task:

1. Importare uno schema
2. Indicizzare alcune voci
3. Aggiungere oggetti

2.2.1. Schema Samba

Affinché OpenLDAP possa essere usato come backend da Samba, logicamente, è necessario che il DIT possa usare correttamente gli attributi che descrivono i dati Samba: questi attributi possono essere ottenuti per mezzo di uno schema Samba LDAP, come sarà indicato nel prosieguo.

Per maggiori informazioni sugli schemi e la loro installazione, consultare *Sezione 1.4, «Modificare il database di configurazione di slapd» [98]*.

1. Lo schema si trova nel pacchetto appena installato samba-doc: è necessario decomprimerlo e copiarlo nella directory `/etc/ldap/schema`:

```
sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema
```

```
sudo gzip -d /etc/ldap/schema/samba.schema.gz
```

2. Creare un file di configurazione `schema_convert.conf` contenente quanto segue:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/ldapns.schema
include /etc/ldap/schema/pmi.schema
include /etc/ldap/schema/samba.schema
```

3. Creare una directory `ldif_output` in cui salvare l'output.
4. Determinare l'indice dello schema:

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | grep samba,cn=schema

dn: cn={14}samba,cn=schema,cn=config
```

5. Convertire lo schema nel formato LDIF:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \ ldap:///cn={14}samba,cn=schema,cn=config
```

6. Modificare il file generato `cn=samba.ldif` eliminando le informazioni dell'indice, per arrivare a:

```
dn: cn=samba,cn=schema,cn=config
...
cn: samba
```

   Eliminare le righe in fondo:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

   I valori degli attributi variano.

7. Aggiungere il nuovo schema:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=samba.ldif
```

Per interrogare e visualizzare questo nuovo schema:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config 'cn=*samba*'
```

2.2.2. Indici Samba

Ora che slapd conosce gli attributi Samba, è possibile impostare alcuni indici basati su di essi. Indicizzare le voci è un modo per migliorare le prestazioni quando un client esegue una ricerca condizionata sul DIT.

Creare il file `samba_indices.ldif` contenente quanto segue:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

Usare l'utilità ldapmodify per caricare i nuovi indici:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f samba_indices.ldif
```

Se tutto è andato a buon fine, dovrebbe essere possibile visualizzare i nuovi indici utilizzando ldapsearch:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H \ ldapi:/// -b cn=config olcDatabase={1}hdb olcDbIndex
```

2.2.3. Aggiungere oggetti Samba LDAP

Next, configure the smbldap-tools package to match your environment. The package is supposed to come with a configuration helper script (smbldap-config.pl, formerly configure.pl) that will ask questions about the needed options but there is a *bug*[37] whereby it is not installed (but found in the source code; 'apt-get source smbldap-tools').

[37] https://bugs.launchpad.net/serverguide/+bug/997172

To manually configure the package you need to create and edit the files `/etc/smbldap-tools/smbldap.conf` and `/etc/smbldap-tools/smbldap_bind.conf`.

The smbldap-populate script will then add the LDAP objects required for Samba. It is a good idea to first make a backup of your DIT using slapcat:

```
sudo slapcat -l backup.ldif
```

Una volta effettuato il backup, procedere a inserire i dati nella directory:

```
sudo smbldap-populate
```

È possibile creare un file LDIF contenente i nuovi oggetti Samba eseguendo **sudo smbldap-populate -e samba.ldif**: in questo modo, è possibile visualizzare le modifiche per assicurarsi che tutto sia corretto. In tal caso, eseguire nuovamente lo script senza l'opzione «-e»; in alternativa, è possibile utilizzare il file LDIF per importare i dati normalmente.

La directory LDAP ora ha le informazioni necessarie per autenticare gli utenti Samba.

2.3. Configurare Samba

Sono disponibili diversi metodi per configurare Samba, per maggiori informazioni consultare *Capitolo 18, Reti Windows [277]*. Per configurare Samba all'uso di LDAP, modificare il suo file di configurazione `/etc/samba/smb.conf`, commentando il parametro predefinito *passdb backend* e aggiungendo alcuni parametri riferiti a LDAP:

```
#   passdb backend = tdbsam

# LDAP Settings
   passdb backend = ldapsam:ldap://hostname
   ldap suffix = dc=example,dc=com
   ldap user suffix = ou=People
   ldap group suffix = ou=Groups
   ldap machine suffix = ou=Computers
   ldap idmap suffix = ou=Idmap
   ldap admin dn = cn=admin,dc=example,dc=com
   ldap ssl = start tls
   ldap passwd sync = yes
...
   add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

Modificare i valori in modo che rispecchino il proprio ambiente di lavoro.

Riavviare samba per abilitare le nuove impostazioni:

```
sudo restart smbd
sudo restart nmbd
```

Samba ora necessita di conoscere la password di amministrazione di LDAP (quella impostata durante l'installazione del pacchetto slapd):

```
sudo smbpasswd -w PASSWORD
```

Se sono già presenti degli utenti LDAP e si vuole includerli nel nuovo LDAP integrato con Samba, è necessario naturalmente che questi siano dotati di alcuni attributi supplementari. L'utilità smbpasswd è in grado di fare questo (l'host dovrà poter visualizzare - contare - questi utenti via NSS; installare e configurare libnss-ldapd o libnss-ldap):

```
sudo smbpasswd -a NOME_UTENTE
```

Viene chiesta una password dell'utente: sarà considerata come la nuova password per quell'utente, è possibile sceglierla identica a quella precedente.

Per gestire account utente, di gruppo o di macchina, usare le utilità del pacchetto smbldap-tools package. Alcuni esempi:

- Per aggiungere un nuovo utente:

  ```
  sudo smbldap-useradd -a -P NOME_UTENTE
  ```

  L'opzione *-a* aggiunge gli attributi Samba, l'opzione *-P* invoca l'utilità smbldap-passwd dopo aver creato l'utente, consentendo di inserire una password per quest'ultimo.

- Per rimuovere un utente:

  ```
  sudo smbldap-userdel NOME_UTENTE
  ```

  Nel comando precedente, usare l'opzione *-r* per rimuovere la directory home dell'utente.

- Per aggiungere un gruppo:

  ```
  sudo smbldap-groupadd -a NOME_GRUPPO
  ```

  Come per smbldap-useradd, l'opzione *-a* aggiunge gli attributi Samba.

- Per aggiungere un utente già esistente a un gruppo:

  ```
  sudo smbldap-groupmod -m NOME_UTENTE NOME_GRUPPO
  ```

  Con l'opzione *-m* è possibile aggiungere più di un utente alla volta, elencandoli come valori separati da virgola.

- Per rimuovere un utente da un gruppo:

  ```
  sudo smbldap-groupmod -x NOME_UTENTE NOME_GRUPPO
  ```

- Per aggiungere un account macchina:

```
sudo smbldap-useradd -t 0 -w NOME_UTENTE
```

Sostituire *NOME_UTENTE* con il nome della workstation. L'opzione *-t 0* crea un account macchina immediatamente, mentre *-w* indica di creare l'utente come account macchina. Notare che il parametro *add machine script* in `/etc/samba/smb.conf` è stata modificata per usare smbldap-useradd.

Nel pacchetto smbldap-tools sono disponibili utilità non trattate in questo documento. Ecco un elenco completo:

smbldap-groupadd[38]
smbldap-groupdel[39]
smbldap-groupmod[40]
smbldap-groupshow[41]
smbldap-passwd[42]
smbldap-populate[43]
smbldap-useradd[44]
smbldap-userdel[45]
smbldap-userinfo[46]
smbldap-userlist[47]
smbldap-usermod[48]
smbldap-usershow[49]

2.4. Risorse

- Per ulteriori informazioni sull'installazione e configurazione di Samba, consultare *Capitolo 18, Reti Windows [277]* in questa guida.
- LDAP e SAMBA sono trattati diffusamente nella *Samba HOWTO Collection*[50] upstream.
- In relazione a quanto sopra riportato, consultare in modo particolare la *sezione passdb*[51].
- Sebbene datato (2007) *Linux Samba-OpenLDAP HOWTO*[52] contiene note preziose.
- La pagina principale della *documentazione della comunità su Samba*[53] contiene moltissimi link ad articoli che possono risultare utili.

---

[38] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupadd.8.html
[39] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupdel.8.html
[40] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupmod.8.html
[41] http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupshow.8.html
[42] http://manpages.ubuntu.com/manpages/en/man8/smbldap-passwd.8.html
[43] http://manpages.ubuntu.com/manpages/en/man8/smbldap-populate.8.html
[44] http://manpages.ubuntu.com/manpages/en/man8/smbldap-useradd.8.html
[45] http://manpages.ubuntu.com/manpages/en/man8/smbldap-userdel.8.html
[46] http://manpages.ubuntu.com/manpages/en/man8/smbldap-userinfo.8.html
[47] http://manpages.ubuntu.com/manpages/en/man8/smbldap-userlist.8.html
[48] http://manpages.ubuntu.com/manpages/en/man8/smbldap-usermod.8.html
[49] http://manpages.ubuntu.com/manpages/en/man8/smbldap-usershow.8.html
[50] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
[51] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html
[52] http://download.gna.org/smbldap-tools/docs/samba-ldap-howto/
[53] https://help.ubuntu.com/community/Samba#samba-ldap

3. Kerberos

Kerberos è un sistema di autenticazione di rete basato sul principio di un «agente» terzo fidato.
Le altre due parti sono l'utente e il servizio a cui l'utente vuole autenticarsi. Non tutti i servizi e le applicazioni possono usare Kerberos, ma quelle che ne sono in grado, consentono di portare la rete a essere un SSO (Single Sign On).

Questa sezione spiega come installare e configurare un server Kerberos, fornendo alcuni esempi di configurazione.

3.1. Panoramica

Se si è nuovi di Kerberos, ci sono alcuni termini che è bene comprendere prima di procedere. Molti di questi termini potrebbero essere simili ad altri concetti di altri ambienti più familiari.

- *Principal*: qualsiasi utente, computer e servizio fornito da server deve essere definito come «Kerberos principal».
- *Istanze*: usate dai principal di servizio e da quelli amministrativi.
- *Realms:*: il «reame» unico di controllo fornito dall'installazione di Kerberos. Occorre considerarlo alla stregua del dominio o del gruppo al quale appartengono sia l'host che l'utente. Per convenzione il reame dovrebbe essere scritto in maiuscolo: per impostazione predefinita Ubuntu usa come reame il dominio DNS convertito in maiuscolo (EXAMPLE.COM).
- *Key Distribution Center* (KDC): consiste di tre parti, un database di tutti i principal, il server di autenticazione e il server che garantisce i ticket. Per ogni reame deve esserci almeno un KDC.
- *Ticket Granting Ticket* (TGT): emesso dallo «Authentication Server» (AS), il «Ticket Granting Ticket» è cifrato con la password dell'utente ed è quindi noto solo all'utente e al KDC.
- *Ticket Granting Server* (TGS): emette i ticket su richiesta dei client.
- *Ticket:*: conferma l'identità dei due principal. Uno è l'utente e l'altro il servizio richiesto. Il ticket stabilisce una chiave di cifratura usata per garantire la sicurezza della comunicazione durante la fase di autenticazione.
- *File keytab*: sono file estratti dal KDC e contengono le chiavi di cifratura per un servizio o un host.

Per riassumere, un reame ha almeno un KDC, preferibilmente due per ridondanza, che contiene un database di Principal. Quando un utente accede in una workstation configurata per l'autenticazione Kerberos, il KDC emette un TGT (Ticket Granting Ticket). Se le informazioni fornite dall'utente corrispondono, l'utente viene autenticato e può richiedere i ticket per i servizi Kerberos da un TGS (Ticket Granting Server). I ticket consentono all'utente di autenticarsi al servizio senza dover fornire altri nome utente e password.

3.2. Server Kerberos

3.2.1. Installazione

In seguito, verrà creato un dominio MIT Kerberos con le seguenti caratteristiche (modificarle in base alle proprie esigenze):

- *Reame:* EXAMPLE.COM
- *KDC primario:* kdc01.example.com (192.168.0.1)
- *KDC secondario:* kdc02.example.com (192.168.0.2)
- *Utente principal:* steve
- *Amministratore principal:* steve/admin

Si raccomanda *vivamente* che gli utenti autenticati dalla rete abbiano un UID in un intervallo diverso (per esempio, partendo da 5000) da quello degli utenti locali.

Prima di installare il server Kerberos, è necessario disporre di un server DNS correttamente configurato per il proprio dominio. Dato che il reame Kerberos per convenzione corrisponde al dominio, questa sezione utilizza il dominio *EXAMPLE.COM* configurato come indicato in *Sezione 2.3, «Server primario» [143]*, nella documentazione su DNS.

Kerberos, inoltre, è un protocollo basato sul tempo. Se l'ora locale tra il client e il server differisce di più di 5 minuti (impostazione predefinita), la workstation non potrà autenticarsi. Per correggere questo problema, tutti gli host dovrebbero sincronizzare il proprio orario usando il medesimo server *Network Time Protocol (NTP)*. Per maggiori informazioni, consultare la sezione *Sezione 4, «Sincronizzazione del tempo con NTP» [51]*.

Il primo passo per creare un reame Kerberos consiste nell'installare i pacchetti krb5-kdc e krb5-admin-server. In un terminale, digitare:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

Alla fine dell'installazione viene chiesto di fornire un nome host per i server Kerberos e Admin del reame, che potrebbero essere anche lo stesso server.

Per impostazione predefinita, il reame viene creato con lo stesso nome del dominio di KDC.

Creare il reame con l'utilità kdb5_newrealm:

```
sudo krb5_newrealm
```

3.2.2. Configurazione

Le domande poste durate l'installazione sono usate per impostare il file `/etc/krb5.conf`. Per modificare le impostazioni del KDC (Key Distribution Center), basta modificare il file e riavviare il

demone krb5-kdc. Se è necessario riconfigurare Kerberos da zero, magari per cambiare il nome del reame, digitare:

```
sudo dpkg-reconfigure krb5-kdc
```

1. Ora che il KDC è in esecuzione, è necessario avere un utente amministratore -- l'*admin principal*; si raccomanda di usare un nome utente diverso da quello usato giornalmente per le normali operazioni al computer. Usando l'utilità kadmin.local, digitare in un terminale:

   ```
   sudo kadmin.local
   Authenticating as principal root/admin@EXAMPLE.COM with password.
   kadmin.local: addprinc steve/admin
   WARNING: no policy specified for steve/admin@EXAMPLE.COM; defaulting to no policy
   Enter password for principal "steve/admin@EXAMPLE.COM":
   Re-enter password for principal "steve/admin@EXAMPLE.COM":
   Principal "steve/admin@EXAMPLE.COM" created.
   kadmin.local: quit
   ```

   Nell'esempio precedente *steve* è il *Principal*, */admin* è un'*Istanza* e *@EXAMPLE.COM* indica il reame. Il Principal *«giornaliero»*, cioè l'*utente principal*, è *steve@EXAMPLE.COM* e dovrebbe avere i diritti di un utente normale.

   Sostituire *EXAMPLE.COM* e *steve* con il proprio reame e il nome utente dell'amministratore.

2. Il nuovo utente amministratore necessita dei permessi ACL (Access Control List) corretti, configurati tramite il file `/etc/krb5kdc/kadm5.acl`:

   ```
   steve/admin@EXAMPLE.COM        *
   ```

   Questa voce garantisce a *steve/admin* la possibilità di eseguire qualsiasi operazione su tutti i principal nel reame. È possibile configurare dei principal con privilegi più limitati, il che può essere conveniente ove sia necessaria la figura di un amministratore principal che possa essere utilizzato da personale meno esperto in client Kerberos. Per maggiori dettagli, consultare la pagina del manuale *kadm5.acl*.

3. Riavviare krb5-admin-server affinché le nuove ACL abbiano effetto:

   ```
   sudo service krb5-admin-server restart
   ```

4. Il nuovo utente può essere provato con l'utilità kinit:

   ```
   kinit steve/admin
   steve/admin@EXAMPLE.COM's Password:
   ```

   Una volta inserita la password, usare l'utilità klist per visualizzare le informazioni riguardo il TGT (Ticket Granting Ticket):

```
klist
Credentials cache: FILE:/tmp/krb5cc_1000
        Principal: steve/admin@EXAMPLE.COM

  Issued           Expires          Principal
Jul 13 17:53:34  Jul 14 03:53:34  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

Dove il nome del file cache `krb5cc_1000` è composto dal prefisso `krb5cc_` e dall'identificativo dell'utente (UID), in questo caso `1000`. Potrebbe essere necessario aggiungere una voce nel file `/etc/hosts` per il KDC, per esempio:

```
192.168.0.1   kdc01.example.com       kdc01
```

Sostituire *192.168.0.1* con l'indirizzo IP del KDC: questo accade normalmente quando il reame Kerberos comprende diverse reti separate da router.

5. Il migliore modo per consentire ai client di determinare automaticamente il KDC per il reame, è usare i record DNS SRV. Aggiungere quanto segue al file `/etc/named/db.example.com`:

```
_kerberos._udp.EXAMPLE.COM.     IN SRV 1  0 88  kdc01.example.com.
_kerberos._tcp.EXAMPLE.COM.     IN SRV 1  0 88  kdc01.example.com.
_kerberos._udp.EXAMPLE.COM.     IN SRV 10 0 88  kdc02.example.com.
_kerberos._tcp.EXAMPLE.COM.     IN SRV 10 0 88  kdc02.example.com.
_kerberos-adm._tcp.EXAMPLE.COM. IN SRV 1  0 749 kdc01.example.com.
_kpasswd._udp.EXAMPLE.COM.      IN SRV 1  0 464 kdc01.example.com.
```

Sostituire *EXAMPLE.COM*, *kdc01* e *kdc02* con il nome del proprio dominio, il KDC primario e quello secondario.

Consultare *Capitolo 8, DNS (Domain Name Service) [140]* per le istruzioni sulla configurazione di DNS.

Il reame Kerberos è ora pronto per autenticare i client.

3.3. KDC secondario

Una volta ottenuto un KDC (Key Distribution Center) all'interno della rete, è utile avere anche un KDC secondario nel caso in cui quello primario non fosse più disponibile. Inoltre, se i client Kerberos sono in reti diverse (eventualmente separate da router che usano NAT), è opportuno collocare un KDC secondario in ognuna di queste reti.

1. Per prima cosa installare il pacchetto e quando vengono chiesti i nomi di Kerberos e Admin, inserire il nome del KDC primario:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

2. Una volta installato il pacchetto, creare il KDC secondario. Da un terminale, digitare:

```
kadmin -q "addprinc -randkey host/kdc02.example.com"
```

Una volta eseguiti i comandi kadmin viene chiesto la propria password *NOME_UTENTE/ADMIN@EXAMPLE.COM*.

3. Estrarre il file *keytab*:

```
kadmin -q "ktadd -norandkey -k keytab.kdc02 host/kdc02.example.com"
```

4. Dovrebbe esserci un file `keytab.kdc02` nella directory corrente, spostare il file in `/etc/krb5.keytab`:

```
sudo mv keytab.kdc02 /etc/krb5.keytab
```

Se il percorso a `keytab.kdc02` è diverso, modificarlo in base al proprio caso.

È possibile elencare tutti i principal presenti in un file Keytab, utile durante la risoluzione dei problemi, con l'utilità klist:

```
sudo klist -k /etc/krb5.keytab
```

L'opzione -k indica che il file è keytab.

5. Dovrebbe esserci un file `kpropd.acl` in ogni KDC che presenti tutti i KDC del reame. Per esempio, sia sul KDC primario che secondario, creare un file `/etc/krb5kdc/kpropd.acl`:

```
host/kdc01.example.com@EXAMPLE.COM
host/kdc02.example.com@EXAMPLE.COM
```

6. Creare un database vuoto nel *KDC secondario*:

```
sudo kdb5_util -s create
```

7. Avviare il demone kpropd che resterà in ascolto per le connessioni dall'utilità kprop. kprop è usato per trasferire i file di dump:

```
sudo kpropd -S
```

8. Da un terminale dal *KDC primario*, creare un file di dump del database principale:

```
sudo kdb5_util dump /var/lib/krb5kdc/dump
```

9. Estrarre il *keytab* del KDC primario e copiarlo in `/etc/krb5.keytab`:

```
kadmin -q "ktadd -k keytab.kdc01 host/kdc01.example.com"
sudo mv keytab.kdc01 /etc/krb5.keytab
```

Assicurarsi che ci sia un *host* per *kdc01.example.com* prima di estrarre il keytab.

10. Usando l'utilità kprop eseguire il push del database sul KDC secondario:

```
sudo kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```

Dovrebbe essere visualizzato un messaggio di *SUCCEEDED* se la propagazione è andata a buon fine. Se si è verificato un errore, per maggiori informazioni, controllare `/var/log/syslog` sul KDC secondario.

Potrebbe esser utile creare anche un'attività cron per aggiornare periodicamente il database sul KDC secondario. Per esempio, il comando seguente esegue il push del database ogni ora (da notare che la riga è stata divisa in due per adattarla al formato di questo documento):

```
# m h dom mon dow command
0 * * * * /usr/sbin/kdb5_util dump /var/lib/krb5kdc/dump &&
/usr/sbin/kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```

11. Sempre nel *KDC secondario*, creare un file *stash* in cui salvare la chiave principale di Kerberos:

```
sudo kdb5_util stash
```

12. Avviare il demone krb5-kdc sul KDC secondario:

```
sudo service krb5-kdc start
```

Il *KDC secondario* dovrebbe ora essere in grado di emettere i ticket per il reame. È possibile verificare ciò fermando il demone krb5-kdc sul KDC primario e usando kinit per richiedere un ticket. Se tutto funziona correttamente, si dovrebbe ricevere un ticket dal KDC secondario, in caso contrario controllare `/var/log/syslog` e `/var/log/auth.log` nel KDC secondario.

3.4. Client Kerberos Linux

Questa sezione spiega come configurare un sistema Linux come un client Kerberos consentendo l'accesso a qualsiasi servizio Kerberos ad accesso effettuato correttamente da parte degli utenti.

3.4.1. Installazione

Per autenticarsi in un reame Kerberos sono necessari i pacchetti krb5-user e libpam-krb5 oltre ad altri non strettamente necessari, ma che semplificano molto la gestione. Per installare questi pacchetti, digitare:

```
sudo apt-get install krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

Il pacchetto auth-client-config consente una semplice configurazione dell'autenticazione PAM per diverse sorgenti e libpam-ccreds memorizza le credenziali di autenticazione consentendo di effettuare

l'accesso anche se il KDC non è disponibile. Questo pacchetto è utile anche per i computer portatili che possono autenticarsi su reti aziendali, ma devono essere in grado di farlo anche al di fuori della rete.

3.4.2. Configurazione

Per configurare il client, in un terminale digitare:

```
sudo dpkg-reconfigure krb5-config
```

Viene quindi chiesto di inserire il nome del reame Kerberos. Inoltre, se non si dispone di un DNS configurato con i record *SRV* di Kerberos, viene richiesto il nome dell'host del KDC e del server amministrativo.

Il comando dpkg-reconfigure aggiunge delle voci al file `/etc/krb5.conf` del proprio reame. Dovrebbero essere disponibili delle voci simili alle seguenti:

```
[libdefaults]
        default_realm = EXAMPLE.COM
...
[realms]
        EXAMPLE.COM = }
                kdc = 192.168.0.1
                admin_server = 192.168.0.1
        }
```

Se si imposta l'UID di ognuno degli utenti autenticati dalla rete a 5000, come suggerito in *Sezione 3.2.1, «Installazione» [126]*, è possibile validare solo quelli che cercano di autenticarsi usando utenti Kerberos con UID > 5000:

```
# Kerberos dovrebbe essere applicato solo agli utenti ldap/kerberos, non a quelli locali. f
```

Questo eviterà che vengano richieste (inesistenti) password Kerberos di utenti autenticati localmente quando si modifica la password con **passwd**.

Per avviare la configurazione, richiedere un ticket usando l'utilità kinit. Per esempio:

```
kinit steve@EXAMPLE.COM
Password for steve@EXAMPLE.COM:
```

Una volta ottenuto un ticket, i dettagli possono essere visualizzati usando klist:

```
klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: steve@EXAMPLE.COM

Valid starting     Expires            Service principal
```

```
07/24/08 05:18:56  07/24/08 15:18:56  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 07/25/08 05:18:57


Kerberos 4 ticket cache: /tmp/tkt1000
klist: You have no tickets cached
```

Usare auth-client-config per configurare il modulo libpam-krb5 affinché richieda un ticket durante la fase di accesso:

```
sudo auth-client-config -a -p kerberos_example
```

Una volta autenticati con successo, si dovrebbe ricevere un ticket.

3.5. Risorse

- Per ulteriori informazioni sulle versioni Kerberos del MIT, consultare il sito web *MIT Kerberos*[54].
- La pagina della *documentazione della comunità su Kerberos*[55] contiene maggiori dettagli.
- Il libro *Kerberos: The Definitive Guide*[56] di O'Reilly è un ottimo punto di riferimento per impostare un server Kerberos.
- Inoltre, fare un giro sui canali IRC *#ubuntu-server* e *#kerberos* su *Freenode*[57], se si hanno domande riguardanti Kerberos.

---

54 http://web.mit.edu/Kerberos/
55 https://help.ubuntu.com/community/Kerberos
56 http://oreilly.com/catalog/9780596004033/
57 http://freenode.net/

4. Kerberos e LDAP

Normalmente Kerberos non viene utilizzato da solo; una volta che un utente è autenticato (Kerberos), è necessario comprendere cosa può fare (autorizzazione), e questo è il compito di programmi come LDAP.

Sostituire un database principale di Kerberos tra due server può essere complicato e aggiunge un ulteriori database all'interno della rete. Il server Kerberos può comunque essere configurato per utilizzare una directory LDAP come database principale. In questa sezione viene descritto come configurare un server Kerberos, primario e secondario, affinché utilizzi OpenLDAP come database principale.

Il seguente esempio dà per scontato che siano installati MIT Kerberos e OpenLDAP.

4.1. Configurare OpenLDAP

Per prima cosa è necessario caricare lo *schema* all'interno del server OpenLDAP collegato ai KDC primario e secondario. I successivi passi qui descritti hanno come presupposto la presenza di un server LDAP di replica configurato tra due server. Per maggiori informazioni su come impostare un server OpenLDAP, consultare *Sezione 1, «Server OpenLDAP» [93]*.

È inoltre richiesto per configurare OpenLDAP all'uso di connessioni TLS e SSL, in modo che il traffico tra il KDC e il server LDAP sia cifrato. Per maggiori informazioni, consultare *Sezione 1.8, «TLS» [107]*.

`cn=admin,cn=config` è un utente creato con diritti di modifica del database ldap, normalmente è l'amministratore ldap; modificare questo valore per adattarlo alle proprie impostazioni.

- Per caricare lo schema all'interno del server LDAP, installare su tale server il pacchetto krb5-kdc-ldap. Da un terminale, digitare:

  ```
  sudo apt-get install krb5-kdc-ldap
  ```

- Estrarre il file `kerberos.schema.gz`:

  ```
  sudo gzip -d /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz
  sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema /etc/ldap/schema/
  ```

- Lo schema *kerberos* deve essere aggiunto all'albero *cn=config*. La procedura per aggiungere un nuovo schema a slapd è descritta anche in *Sezione 1.4, «Modificare il database di configurazione di slapd» [98]*.

  1. Creare un file di configurazione chiamato `schema_convert.conf`, o simile, contenente quanto segue:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/kerberos.schema
```

2. Creare una directory temporanea in cui salvare i file LDIF:

```
mkdir /tmp/ldif_output
```

3. Usare quindi slapcat per convertire i file schema:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s \ "cn={12}kerberos,cn=schema,cn=con
```

Modificare i percorsi e i nomi dei file in base alla proprie esigenze.

4. Modificare il file `/tmp/cn\=kerberos.ldif` generato sistemando i seguenti attributi:

```
dn: cn=kerberos,cn=schema,cn=config
...
cn: kerberos
```

Rimuovere le seguenti righe dalla fine del file:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 18ccd010-746b-102d-9fbe-3760cca765dc
creatorsName: cn=config
createTimestamp: 20090111203515Z
entryCSN: 20090111203515.326445Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20090111203515Z
```

I valori degli attributi possono variare, basta solo assicurarsi che gli attributi siano rimossi.

5. Caricare il nuovo schema con ldapadd:

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=kerberos.ldif
```

6. Aggiungere un indice per l'attributo *krb5principalname*:

```
ldapmodify -x -D cn=admin,cn=config -W
```

```
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: krbPrincipalName eq,pres,sub

modifying entry "olcDatabase={1}hdb,cn=config"
```

7. Infine, aggiornare le ACL (Access Control Lists):

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
replace: olcAccess
olcAccess: to attrs=userPassword,shadowLastChange,krbPrincipalKey by
 dn="cn=admin,dc=example,dc=com" write by anonymous auth by self write by * none
-
add: olcAccess
olcAccess: to dn.base="" by * read
-
add: olcAccess
olcAccess: to * by dn="cn=admin,dc=example,dc=com" write by * read

modifying entry "olcDatabase={1}hdb,cn=config"
```

La directory LDAP è ora pronta come database principale per Kerberos.

4.2. Configurazione KDC primario

Configurato OpenLDAP, è necessario configurare KDC.

- Installare i pacchetti necessari. In un terminale, digitare:

```
sudo apt-get install krb5-kdc krb5-admin-server krb5-kdc-ldap
```

- Modificare `/etc/krb5.conf` aggiungendo le seguenti opzioni all'interno delle sezioni appropriate:

```
[libdefaults]
        default_realm = EXAMPLE.COM

...

[realms]
        EXAMPLE.COM = {
                kdc = kdc01.example.com
                kdc = kdc02.example.com
                admin_server = kdc01.example.com
                admin_server = kdc02.example.com
                default_domain = example.com
                database_module = openldap_ldapconf
        }
```

```
...

[domain_realm]
        .example.com = EXAMPLE.COM


...

[dbdefaults]
        ldap_kerberos_container_dn = dc=example,dc=com

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps://ldap01.example.com ldaps://ldap02.example.com
                ldap_conns_per_server = 5
        }
```

Modificare *example.com*, *dc=example,dc=com*, *cn=admin,dc=example,dc=com* e *ldap01.example.com* con i valori corretti del dominio, dell'oggetto e del server LDAP della propria rete.

- Usare l'utilità kdb5_ldap_util per creare il reame:

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com create -subtrees \ dc=example,dc=com -r EXAMPLE
```

- Creare un file stash della password utilizzata per l'associazione al server LDAP. Questa password è usata con le opzioni *ldap_kdc_dn* e *ldap_kadmin_dn* nel file `/etc/krb5.conf`:

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com stashsrvpw -f \ /etc/krb5kdc/service.keyfile cn
```

- Copiare il certificato della CA dal server LDAP:

```
scp ldap01:/etc/ssl/certs/cacert.pem .
sudo cp cacert.pem /etc/ssl/certs
```

Modificare il file `/etc/ldap/ldap.conf` affinché utilizzi il certificato:

```
TLS_CACERT /etc/ssl/certs/cacert.pem
```

Il certificato deve anche essere copiato nel KDC secondario per consentire la connessione ai server LDAP utilizzando LDAPS.

Ora è possibile aggiungere i principal Kerberos al database LDAP che verranno copiati su tutti gli altri server LDAP di replica. Per aggiungere un principal utilizzando l'utilità kadmin.local, digitare:

```
sudo kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local:  addprinc -x dn="uid=steve,ou=people,dc=example,dc=com" steve
WARNING: no policy specified for steve@EXAMPLE.COM; defaulting to no policy
Enter password for principal "steve@EXAMPLE.COM":
Re-enter password for principal "steve@EXAMPLE.COM":
Principal "steve@EXAMPLE.COM" created.
```

Dovrebbero ora essere aggiunti all'oggetto utente *uid=steve,ou=people,dc=example,dc=com* gli attributi krbPrincipalName, krbPrincipalKey, krbLastPwdChange e krbExtraData. Per verificare che all'utente venga emesso un ticket, utilizzare le utilità kinit e klist.

Se l'oggetto utente è già stato creato, è necessario usare l'opzione *-x dn="..."* per aggiungere gli attributi Kerberos, altrimenti verrà creato un nuovo oggetto *principal* nel sottoalbero del reame.

4.3. Configurazione KDC secondario

La configurazione di un KDC secondario utilizzando il backend LDAP è molto simile alla configurazione tramite l'utilizzo del database Kerberos.

1. Installare i pacchetti necessari. In un terminale digitare:

   ```
   sudo apt-get install krb5-kdc krb5-admin-server krb5-kdc-ldap
   ```

2. Modificare il file `/etc/krb5.conf` affinché utilizzi il backend LDAP:

   ```
   [libdefaults]
           default_realm = EXAMPLE.COM

   ...

   [realms]
           EXAMPLE.COM = {
                   kdc = kdc01.example.com
                   kdc = kdc02.example.com
                   admin_server = kdc01.example.com
                   admin_server = kdc02.example.com
                   default_domain = example.com
                   database_module = openldap_ldapconf
   ```

```
        }

...

[domain_realm]
        .example.com = EXAMPLE.COM

...

[dbdefaults]
        ldap_kerberos_container_dn = dc=example,dc=com

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps://ldap01.example.com ldaps://ldap02.example.com
                ldap_conns_per_server = 5
        }
```

3. Creare il file stash per la password di associazione LDAP:

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com stashsrvpw -f \ /etc/krb5kdc/service.keyfile
```

4. Dal *KDC primario*, copiare il file di stash della *chiave primaria* (`/etc/krb5kdc/.k5.EXAMPLE.COM`) nel KDC secondario. Accertarsi di copiare tale file utilizzando una connessione cifrata come scp o su un supporto fisico.

```
sudo scp /etc/krb5kdc/.k5.EXAMPLE.COM steve@kdc02.example.com:~
sudo mv .k5.EXAMPLE.COM /etc/krb5kdc/
```

Ricordarsi di sostituire *EXAMPLE.COM* con il reame in uso.

5. Dal *KDC secondario*, (ri)avviare solo il server ldap,

```
sudo service slapd restart
```

6. Infine, avviare il demone krb5-kdc:

```
sudo service krb5-kdc start
```

7. Verificare che i due server ldap (e Kerberos in senso lato) siano sincronizzati.

All'interno della propria rete sono quindi disponibili dei KDC ridondanti che assieme ai server LDAP ridondanti permettono l'autenticazione degli utenti anche nel caso in cui un server LDAP, un server Kerberos o uno server LDAP e un server Kerberos non siano più disponibili.

4.4. Risorse

- Maggiori informazioni possono essere trovate nella *Kerberos Admin Guide*[58].
- For more information on kdb5_ldap_util see *Section 5.6*[59] and the *kdb5_ldap_util man page*[60].
- Another useful link is the *krb5.conf man page*[61].
- È possibile consultare anche la *documentazione online della comunità su Kerberos e LDAP*[62].

58 http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Configuring-Kerberos-with-OpenLDAP-back_002dend
59 http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Global-Operations-on-the-Kerberos-LDAP-Database
60 http://manpages.ubuntu.com/manpages/quantal/en/man8/kdb5_ldap_util.8.html
61 http://manpages.ubuntu.com/manpages/quantal/en/man5/krb5.conf.5.html
62 https://help.ubuntu.com/community/Kerberos#kerberos-ldap

Capitolo 8. DNS (Domain Name Service)

Il DNS (Domain Name Service) è un servizio Internet che mappa gli indirizzi IP e i nomi di dominio univoci (FQDN) tra di loro facendo in modo di non dover ricordare gli indirizzi IP. I computer che eseguono DNS sono chiamati *server dei nomi*. Ubuntu è dotato di BIND (Berkley Internet Naming Daemon), il più diffuso programma usato per mantenere un server dei nomi su Linux.

1. Installazione

A un promt di terminale, inserire il seguente comando per installare dns:

```
sudo apt-get install bind9
```

Un pacchetto molto utile per fare test e risolvere problemi legati al DNS nel pacchetto dnsutils: molto spesso questi strumenti sono già installati, ma per controllare installare dnsutils, digitare quanto segue:

```
sudo apt-get install dnsutils
```

2. Configurazione

BIND9 può essere configurato in diversi modi tra cui: come cache per server dei nomi, master principale e master secondario.

- Quando configurato come un server dei nomi cache, BIND9 troverà la risposta alle interrogazioni sui nomi e la archivierà.
- Come server primario, BIND9 legge i dati per una zona da un file ed è autoritativo per quella zona.
- Nella configurazione come server secondario, BIN9 ottiene i dati della zona da un altro server dei nomi per quella zona.

2.1. Panoramica

I file di configurazione di DNS sono archiviati nella directory `/etc/bind`, il file di configurazione principale è `/etc/bind/named.conf`.

La riga *include* specifica il nome del file contenente le opzioni DNS, la riga *directory* nel file `/etc/bind/named.conf.options` indica a DNS dove cercare i file. Tutti i file usati da BIND sono presenti in questa directory.

Il file `/etc/bind/db.root` descrive i server dei nomi «radice» nel mondo. Questi server cambiano col tempo, quindi il file `/etc/bind/db.root` deve essere aggiornato ogni tanto, procedura che viene svolta, solitamente, con gli aggiornamenti al pacchetto bind9. La sezione *zone* definisce un server principale ed è archiviata in un file indicato dall'opzione *file*.

È possibile configurare lo stesso server sia come server dei nomi cache, master primario e secondario. Un server può ricoprire il ruolo di «Start of Authority» (SOA) per una zona, fornendo allo stesso tempo servizi di server secondario per un'altra zona e di cache per gli host della LAN.

2.2. Server dei nomi cache

La configurazione predefinita comporta l'utilizzo come server di cache. È necessario solamente aggiungere gli indirizzi IP dei server DNS del proprio ISP. De-commentare e modificare quanto segue nel file `/etc/bind/named.conf.options`:

```
forwarders {
                1.2.3.4;
                5.6.7.8;
           };
```

Sostituire *1.2.3.4* e *5.6.7.8* con gli indirizzi IP del server di nomi attuale.

Per abilitare la nuova configurazione è necessario riavviare il server DNS. Da un terminale, digitare:

```
sudo service bind9 restart
```

Per maggiori informazioni su come eseguire test su un server cache DNS, consultare *Sezione 3.1.2, «dig» [148]*.

2.3. Server primario

In questa sezione, BIND9 viene configurato come server primario per il dominio *example.com*. Basta sostituire *example.com* con il proprio FQDN (Fully Qualified Domain Name).

2.3.1. File zona forward

Per aggiungere una zona DNS a BIND9, trasformando BIND9 in un server primario, la prima cosa da fare è modificare il file `/etc/bind/named.conf.local`:

```
zone "example.com" {
 type master;
        file "/etc/bind/db.example.com";
};
```

(Note, if bind will be receiving automatic updates to the file as with DDNS, then use `/var/lib/bind/db.example.com` rather than `/etc/bind/db.example.com` both here and in the copy command below.)

Prendere un file zona esistente come modello per creare il file `/etc/bind/db.example.com`:

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

Modificare il nuovo file zona `/etc/bind/db.example.com` cambiando *localhost.* nel FQDN del proprio server, lasciando il «.» alla fine. Modificare *127.0.0.1* con l'indirizzo IP del server di nomi e *root.localhost* con un indirizzo email valido, ma con un «.» al posto del solito simbolo «@», anche in questo caso lasciando il «.» alla fine. Modificare il commento per indicare il dominio per il quale è predisposto questo file.

Creare una *voce A* per il dominio di base, *example.com*. Creare inoltre una *voce A* per *ns.example.com*, il server di nomi in questo esempio:

```
;
; BIND data file for example.com
;
$TTL 604800
@ IN SOA example.com. root.example.com. (
                              2 ; Serial
                         604800 ; Refresh
                          86400 ; Retry
                        2419200 ; Expire
                         604800 ) ; Negative Cache TTL
IN A 192.168.1.10
;
```

```
@ IN NS ns.example.com.
@ IN A 192.168.1.10
@ IN AAAA ::1
ns IN A 192.168.1.10
```

È necessario incrementare il numero *Serial* ogni volta che vengono apportate modifiche al file zona. Se vengono eseguite molteplici modifiche prima di riavviare BIND, incrementare il valore solo una volta.

Ora è possibile aggiungere voci DNS alla fine del file zona. Per maggiori informazioni, consultare la *Sezione 4.1, «Tipi di record comuni» [152]*.

Molti amministratori usano come valore per Serial la data dell'ultima modifica, come *2012010100* in cui si ha AAAAMMGGSS (dove *SS* è il valore Serial).

Modificato il file zona, è necessario riavviare BIND9 affinché le modiche vengano applicate.

```
sudo service bind9 restart
```

2.3.2. File zona reverse

Una volta configurata la zona e la risoluzione dei nomi con un indirizzo IP, è necessaria anche una zona *Reverse*. Una zona «Reverse» consente a DNS di trasformare un indirizzo in un nome.

Modificare il file /etc/bind/named.conf.local aggiungendo quanto segue:

```
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
```

Sostituire *1.168.192* con i primi tre valori dell'indirizzo della rete che si sta usando. Inoltre, chiamare il file zona `/etc/bind/db.192` in modo appropriato, in modo tale che rispecchi il primo ottetto della propria rete.

Creare il file `/etc/bind/db.192`:

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

Quindi modificare `/etc/bind/db.192` cambiando le stesse opzioni di `/etc/bind/db.example.com`:

```
;
; BIND reverse data file for local 192.168.1.XXX net
;
$TTL 604800
@ IN SOA ns.example.com. root.example.com. (
                              2 ; Serial
                         604800 ; Refresh
```

```
                         86400 ; Retry
                       2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@ IN NS ns.
10 IN PTR ns.example.com.
```

Anche il valore *Serial* nella zona «reverse» deve essere aumentato a ogni modifica. Per ogni *voce A* configurata in `/etc/bind/db.example.com`, cioè per un diverso indirizzo, è necessario creare una *voce PTR* in `/etc/bind/db.192`.

Dopo aver creato il file zona «reverse», riavviare BIND9:

```
sudo service bind9 restart
```

2.4. Server secondario

Una volta configurato un *server primario*, un *server secondario* è necessario per mantenere la disponibilità del dominio nel caso in cui quello primario non fosse più disponibile.

Per prima cosa, nel server primario («Primary Master«), deve essere consentita la zona «transfer». Aggiungere l'opzione *allow-transfer* alle definizioni delle zone «Forward» e «Reverse» in `/etc/bind/named.conf.local`:

```
zone "example.com" {
        type master;
 file "/etc/bind/db.example.com";
        allow-transfer { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
 allow-transfer { 192.168.1.11; };
};
```

Sostituire *192.168.1.11* con l'indirizzo IP del server di nomi secondario.

Riavviare BIND9 nel server primario:

```
sudo service bind9 restart
```

Quindi, in quello secondario («Secondary Master»), installare il pacchetto bind9 come fatto per il server primario, quindi modificare il file `/etc/bind/named.conf.local` e aggiungere le seguenti dichiarazioni per le zone «Forward» e «Reverse»:

```
zone "example.com" {
 type slave;
        file "db.example.com";
        masters { 192.168.1.10; };
};

zone "1.168.192.in-addr.arpa" {
 type slave;
        file "db.192";
        masters { 192.168.1.10; };
};
```

Sostituire *192.168.1.10* con l'indirizzo IP del server dei nomi primario.

Riavviare BIND9 nel server secondario:

```
sudo service bind9 restart
```

In `/var/log/syslog` dovrebbe essere visualizzato qualcosa del genere (alcune righe sono state divise per adattarle al formato di questo documento):

```
client 192.168.1.10#39448: received notify for zone '1.168.192.in-addr.arpa'
zone 1.168.192.in-addr.arpa/IN: Transfer started.
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
 connected using 192.168.1.11#37531
zone 1.168.192.in-addr.arpa/IN: transferred serial 5
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
 Transfer completed: 1 messages,
6 records, 212 bytes, 0.002 secs (106000 bytes/sec)
zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 5)

client 192.168.1.10#20329: received notify for zone 'example.com'
zone example.com/IN: Transfer started.
transfer of 'example.com/IN' from 192.168.1.10#53: connected using 192.168.1.11#38577
zone example.com/IN: transferred serial 5
transfer of 'example.com/IN' from 192.168.1.10#53: Transfer completed: 1 messages,
8 records, 225 bytes, 0.002 secs (112500 bytes/sec)
```

Nota: Una zona è trasferita solo se il numero *Serial* del server primario è maggiore di quello del server secondario. Per ottenere che il server primario DSN notifichi ai server secondari DNS i cambiamenti di zona, aggiungere *also-notify { indirizzo IP; };* in `/etc/bind/named.conf.local` come mostrato nel seguente esempio:

```
zone "example.com" {
 type master;
 file "/etc/bind/db.example.com";
 allow-transfer { 192.168.1.11; };
 also-notify { 192.168.1.11; };
```

```
 };

zone "1.168.192.in-addr.arpa" {
 type master;
 file "/etc/bind/db.192";
 allow-transfer { 192.168.1.11; };
 also-notify { 192.168.1.11; };
 };
```

La directory predefinita per file di zona non-autoritativi è `/var/cache/bind/`. Questa directory è configurata anche in AppArmor per consentirne la scrittura da parte del demone named. Per maggiori informazioni, consultare *Sezione 4, «AppArmor» [168]*.

3. Risoluzione problemi

Questa sezione descrive i metodi per determinare le cause dei problemi che si possono verificare con DNS e BIND9.

3.1. Test

3.1.1. resolv.conf

Il primo passo per verificare BIND9 consiste nell'aggiungere l'indirizzo IP del server di nomi in un risolutore di host. Il server dei nomi primario dovrebbe essere configurato così come un altro host per verificare il tutto. Modificare il file `/etc/resolv.conf` e aggiungere quanto segue:

```
nameserver 192.168.1.10
nameserver 192.168.1.11
```

Potrebbe essere necessario aggiungere anche l'indirizzo IP del server di nomi secondario nel caso in cui il primario non fosse più disponibile.

3.1.2. dig

Se è stato installato il pacchetto dnsutils, è possibile configurare l'utilità di ricerca DNS dig:

- Una volta installato BIND9 usare dig sull'interfaccia di loopback per assicurarsi che sia in ascolto sulla porta 53. Da un terminale digitare:

  ```
  dig -x 127.0.0.1
  ```

  L'output del comando dovrebbe essere simile al seguente:

  ```
  ;; Query time: 1 msec
  ;; SERVER: 192.168.1.10#53(192.168.1.10)
  ```

- Se BIND9 è stato configurato come un server di *cache*, eseguire «dig» su un dominio esterno per verificare il tempo dell'interrogazione:

  ```
  dig ubuntu.com
  ```

  Prestare attenzione al tempo dell'interrogazione verso la fine dell'output:

  ```
  ;; Query time: 49 msec
  ```

  Dopo una seconda esecuzione del comando si dovrebebro vedere dei miglioramenti:

  ```
  ;; Query time: 1 msec
  ```

3.1.3. ping

Per dimostrare come le applicazioni utilizzino i DNS per interpretare un nome host, usare l'utilità ping per inviare una richiesta eco ICMP. Da un terminale digitare:

```
ping example.com
```

In questo modo si verifica che il server dei nome sia in grado di interpretare il nome *ns.example.com* in un indirizzo IP. L'output del comando dovrebbe essere simile a quanto segue:

```
PING ns.example.com (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.800 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.813 ms
```

3.1.4. named-checkzone

Un ottimo modo per provare i propri file zona consiste nell'usare l'utilità named-checkzone installata con il pacchetto bind9. Questa utilità consente di verificare che la configurazione sia corretta prima di riavviare BIND9 e consentendo di apportare delle modifiche.

- Per provare il file zona «Forward», in un terminale, digitare quanto segue:

  ```
  named-checkzone example.com /etc/bind/db.example.com
  ```

  Se tutto è stato configurato correttamente, si dovrebbe vedere un output simile a questo:

  ```
  zone example.com/IN: loaded serial 6
  OK
  ```

- Analogamente, per verificare il file zona «Reverse», digitare quanto segue:

  ```
  named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192
  ```

  L'output dovrebbe essere simile a quanto segue:

  ```
  zone 1.168.192.in-addr.arpa/IN: loaded serial 3
  OK
  ```

Il valore *Serial* del proprio file zona probabilmente sarà diverso.

3.2. Registrazione

BIND9 dispone di diverse configurazione per la registrazione degli eventi. Le due opzioni principali sono: *channel* che configura dove vengono salvate le registrazioni e l'opzione *category* che determina quali informazioni registrare.

Se non viene configurata alcuna opzione di registrazione, quella predefinita è:

```
logging {
     category default { default_syslog; default_debug; };
     category unmatched { null; };
};
```

Questa sezione descrive come configurare BIND9 affinché invii i messaggi di *debug* relativi alle interrogazioni DNS in un file diverso.

- Per prima cosa è necessario configurare un canale per specificare quale a quale file inviare i messaggi. Modificare quindi il file `/etc/bind/named.conf.local` e aggiungere quanto segue:

```
logging {
    channel query.log {
        file "/var/log/query.log";
        severity debug 3;
    };
};
```

- Configurare una categoria per inviare tutte le interrogazioni DNS al file:

```
logging {
    channel query.log {
        file "/var/log/query.log";
        severity debug 3;
    };
    category queries { query.log; };
};
```

L'opzione *debug* può essere impostata tra 1 e 3. Se non viene specificato alcun livello, viene considerato quello predefinito, cioè 1.

- Dato che il demone *named* viene eseguito come l'utente *bind*, è necessario creare il file `/var/log/query.log` e modificarne il proprietario:

```
sudo touch /var/log/query.log
sudo chown bind /var/log/query.log
```

- Prima che il demone named possa scrivere nel nuovo file di registrazione, il profilo AppArmor deve esser aggiorato. Per prima cosa modificare `/etc/apparmor.d/usr.sbin.named` e aggiungere:

```
/var/log/query.log w,
```

Quindi ricaricare il profilo:

```
cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
```

Per maggiori informazioni riguardo AppArmor, consultare la *Sezione 4, «AppArmor» [168]*.

- Riavviare BIND9 affinché le modifiche abbiano effetto:

```
sudo service bind9 restart
```

Dovrebbe essere possibile vedere il file `/var/log/query.log` riempirsi con le informazioni relative alle interrogazioni. Per maggio informazioni sulle opzioni di registrazione di BIND9, consultare la *Sezione 4.2, «Ulteriori informazioni» [152]*.

4. Riferimenti

4.1. Tipi di record comuni

Questa sezione descrive i più comuni tipi di record DNS.

- Record *A*: mappa un indirizzo IP con un nome host.

```
www      IN    A      192.168.1.12
```

- Record *CNAME*: usato per creare un alias di un record «A» esistente. Non è possibile creare un record CNAME che punti a un altro record CNAME.

```
web     IN    CNAME  www
```

- Record *MX*: usato per definire dove dovrebbero essere inviate le email. Deve puntare a un record A, non a uno CNAME.

```
        IN    MX  1   mail.example.com.
mail    IN    A       192.168.1.13
```

- Record *NS*: usato per definire quali server dispongono di copie di una zona. Deve puntare a un record A, non a un CNAME. Qui vengono definiti i server primario e secondario.

```
        IN NS ns.example.com.
        IN NS ns2.example.com.
ns IN A 192.168.1.10
ns2 IN A 192.168.1.11
```

4.2. Ulteriori informazioni

- Il *DNS HOWTO*[1] dispone di maggiori informazioni sulla configurazione di BIND9.
- Per un approfondimento di *DNS* e BIND9, consultare *Bind9.net*[2].
- *DNS and BIND*[3] è un libro molto comune giunto ormai alla quinta edizione.
- Un ottimo posto per richiedere assistenza riguardo BIND9, e per partecipare nella comunità di Ubuntu Server, è il canale IRC *#ubuntu-server* su *freenode*[4].
- Consultare anche la *documentazione di bind9 online*[5].

1 http://www.tldp.org/HOWTO/DNS-HOWTO.html
2 http://www.bind9.net/
3 http://www.oreilly.com/catalog/dns5/index.html
4 http://freenode.net
5 https://help.ubuntu.com/community/BIND9ServerHowto

Capitolo 9. Sicurezza

La sicurezza deve essere sempre considerata come uno degli aspetti più importanti durante l'installazione, lo sviluppo e l'uso di un sistema. Anche se un'installazione base di Ubuntu offre un livello di sicurezza sufficientemente elevato per l'utilizzo immediato su Internet, è importante avere una buona conoscenza della sicurezza del proprio sistema in base a come verrà usato in produzione.

This chapter provides an overview of security related topics as they pertain to Ubuntu 12.10 Server Edition, and outlines simple measures you may use to protect your server and network from any number of potential security threats.

1. Gestione utenti

L'amministrazione degli utenti è una parte critica per il mantenimento di un sistema sicuro. Utenti poco esperti con privilegi di amministrazione spesso sono la causa della compromissione di sistemi. Pertanto, è importante capire come proteggere il proprio server tramite delle semplici ed efficaci tecniche di gestione degli account utente.

1.1. Dove è l'utente root?

Gli sviluppatori di Ubuntu hanno deciso di disattivare in modo predefinito l'account di amministrazione (root) in tutte le installazioni di Ubuntu. Questo non significa che l'account root sia stato eliminato o che non sia più accessibile, è stata impostata una password che non corrisponde ad alcun possibile valore codificato, pertanto, l'accesso come root non è direttamente possibile.

Gli utenti sono incoraggiati a utilizzare lo strumento sudo per svolgere i compiti di amministrazione di sistema. Lo strumento sudo permette a un utente autorizzato di elevare temporaneamente i propri privilegi usando la propria password, invece di dover conoscere direttamente la password di root. Questo semplice, ma efficace, metodo cerca di fornire responsabilità per tutte le azioni degli utenti e dà all'amministratore un controllo granulare sulle azioni che un utente può eseguire con tali privilegi.

- Se per qualche ragione è necessario abilitare l'account root, basta assegnargli semplicemente una password:

  Configurations with root passwords are not supported.

  ```
  sudo passwd
  ```

  Il programma «sudo» chiederà di inserire la propria password e successivamente di inserirne una nuova per l'account root:

  ```
  [sudo] password for NOME_UTENTE: (inserire la propria password)
  Inserire nuova password UNIX: (inserire una nuova password per root)
  Reinserire la nuova password UNIX: (reinserire la nuova password per root)
  passwd: password updated successfully
  ```

- Per disabilitare l'account root, utilizzare la seguente sintassi per passwd:

  ```
  sudo passwd -l root
  ```

- Per maggiori informazioni riguardo sudo, consultarne il manuale:

  ```
  man sudo
  ```

By default, the initial user created by the Ubuntu installer is a member of the group "*sudo*" which is added to the file `/etc/sudoers` as an authorized sudo user. If you wish to give any other account full root access through sudo, simply add them to the *sudo* group.

1.2. Aggiungere e rimuovere utenti

Il processo per la gestione di utenti e gruppi locali è molto intuitivo e differisce poco dalla maggior parte degli altri sistemi GNU/Linux. Ubuntu e altre distribuzioni basate su Debian, incoraggiano l'utilizzo del pacchetto «adduser» per la gestione degli utenti.

- Per aggiungere un nuovo utente, utilizzare i seguenti comandi e seguire le istruzioni per impostare all'account una password e fornire le caratteristiche identificabili come nome, cognome, numero di telefono, ecc...

```
sudo adduser NOME_UTENTE
```

- Per eliminare un utente e il suo gruppo principale, digitare:

```
sudo deluser NOME_UTENTE
```

  Quando si elimina un account utente non viene rimossa la sua cartella home. È decisione dell'amministratore se rimuoverla o no in base alle proprie scelte.

  Ricordare che, se non sono state prese le necessarie precauzioni, ogni nuovo utente aggiunto successivamente con gli stessi UID/GID del precedente proprietario della cartella, avrà accesso a tale cartella.

  È possibile modificare questi valori UID/GID con qualcosa di più appropriato, come per esempio l'account root, e spostare la cartella per evitare futuri conflitti:

```
sudo chown -R root:root /home/NOME_UTENTE/
sudo mkdir /home/archived_users/
sudo mv /home/NOME_UTENTE /home/archived_users/
```

- Per bloccare o sbloccare temporaneamente l'account di un utente, utilizzare, rispettivamente, i seguenti comandi:

```
sudo passwd -l NOME_UTENTE
sudo passwd -u NOME_UTENTE
```

- Per aggiungere o rimuovere un gruppo personalizzato, utilizzare, rispettivamente, i seguenti comandi:

```
sudo addgroup NOME_GRUPPO
sudo delgroup NOME_GRUPPO
```

- Per aggiungere un utente a un gruppo, digitare:

```
sudo adduser NOME_UTENTE NOME_GRUPPO
```

1.3. Sicurezza dei profili utente

Quando viene creato un nuovo utente, l'applicazione «adduser» crea una nuova directory chiamata `/home/NOME_UTENTE`. Il profilo predefinito è modellato secondo i contenuti presenti nella directory `/etc/skel` che contiene tutti i profili di base.

Se il proprio server ospiterà più utenti, è necessario prestare la massima attenzione alle autorizzazioni delle home degli utenti, al fine di garantirne la riservatezza. In modo predefinito, in Ubuntu, le home degli utenti sono create con permessi di lettura e di esecuzione per tutti gli utenti. Questo significa che tutti gli utenti possono visualizzare e accedere al contenuto delle home degli altri utenti, cosa che potrebbe non essere soddisfacente per il proprio ambiente.

- Per verificare i permessi attuali della home degli utenti, utilizzare il seguente comando:

  ```
  ls -ld /home/NOME_UTENTE
  ```

  Il seguente output mostra che la directory `/home/NOME_UTENTE` è accessibile in lettura da parte di tutti gli utenti:

  ```
  drwxr-xr-x 2 nomeutente nomeutente 4096 2007-10-02 20:03 nomeutente
  ```

- È possibile rimuovere il permesso in lettura da tutti con il seguente comando:

  ```
  sudo chmod 0750 /home/NOME_UTENTE
  ```


  Alcuni amministratori utilizzano anche l'opzione per la modifica ricorsiva (-R) di tutte le sotto-cartelle e file della home, ma questo non è necessario e potrebbe inoltre causare degli effetti indesiderati. Modificare i permessi alla cartella principale è più che sufficiente per prevenire degli accessi non autorizzati.

  Un modo più efficiente potrebbe essere quello di modificare direttamente le impostazioni predefinite dell'applicazione adduser sui permessi da assegnare alle home degli utenti appena creati. È sufficiente modificare la variabile `DIR_MODE`, nel file `/etc/adduser.conf`, secondo le proprie esigenze.

  ```
  DIR_MODE=0750
  ```

- Dopo aver corretto opportunamente i permessi di accesso alle directory home come descritto precedentemente, verificare il risultato con il seguente comando:

  ```
  ls -ld /home/NOME_UTENTE
  ```

  Il risultato qui sotto mostra come i permessi di lettura per tutti gli altri utenti siano stati rimossi:

  ```
  drwxr-x--- 2 nomeutente nomeutente 4096 2007-10-02 20:03 nomeutente
  ```

1.4. Politica delle password

Una severa politica delle password è uno dei più importanti aspetti della sicurezza di un sistema. Le più frequenti violazioni di un sistema avvengono tramite attacchi di forza bruta con degli elenchi di parole che statisticamente possono comprende delle parole chiavi utilizzate come password. Se si vuole di offrire un qualsiasi tipo di accesso remoto utilizzando la propria password locale, assicurarsi che la complessità della stessa superi dei limiti minimi di adeguatezza, di impostare delle password con durate massime e controllare frequentemente i propri sistemi di autenticazione.

1.4.1. Lungezza minima di una password

Ubuntu richiede, in modo predefinito, una lunghezza minima per le password pari a 6 caratteri, oltre ad alcuni basilari controlli di entropia. Questi valori sono impostati nel file `/etc/pam.d/common-password`, alla riga:

```
password [success=2 default=ignore] pam_unix.so obscure sha512
```

Per modificare la lunghezza minima delle password impostandola a 8 caratteri, modificare la variabile appropriata con «min=8». Ecco un esempio della modifica:

```
password [success=2 default=ignore] pam_unix.so obscure sha512 min=8
```

I controlli basilari di entropia e le regole sulla lunghezza minima non si applicano all'amministratore mentre utilizza comandi di livello sudo per impostare un nuovo utente.

1.4.2. Scadenza delle password

Quando vengono creati dei nuovi utenti è possibile impostare una durata minima e massima per le loro password, obbligando gli stessi a modificarla alla scadenza.

- Per visualizzare facilmente lo stato attuale di un account utente, utilizzare il seguente comando:

  ```
  sudo chage -l NOME_UTENTE
  ```

  L'output seguente mostra informazioni interessanti sull'account dell'utente, in particolare che non ci sono politiche applicate:

  ```
  Ultimo cambio della password : gen 20, 2008
  Scadenza della password : mai
  Inattività della password : mai
  Scadenza dell'account : mai
  Numero minimo di giorni tra i cambi di password : 0
  Numero massimo di giorni tra i cambi di password : 99999
  Giorni di preavviso prima della scadenza della password : 7
  ```

- Per impostare uno qualsiasi di questi campi, utilizzare il seguente comando e seguire le istruzioni:

```
sudo chage NOME_UTENTE
```

Quello che segue è un esempio di come sia possibile modificare manualmente la data di scadenza dell'account (-E) al 31/01/2008 (inserirla nel formato mm/gg/aaaa o nel formato aaaa/mm/gg), l'età minima della password (-m) a 5 giorni, l'età massima (-M) a 90 giorni, il periodo di inattività (-I) a 5 giorni dopo la scadenza della password e un avvertimento (-W) di 14 giorni prima della scadenza delle password.

```
sudo chage -E 01/31/2011 -m 5 -M 90 -I 30 -W 14 NOME_UTENTE
```

- Per verificare le modifiche, utilizzare lo stesso comando di prima:

```
sudo chage -l NOME_UTENTE
```

Il seguente output mostra i cambiamenti effettuati sull'account:

```
Ultimo cambio della password : gen 20, 2008
Scadenza della password : apr 19, 2008
Inattività della password : mag 19, 2008
Scadenza dell'account : gen 31, 2008
Numero minimo di giorni tra i cambi di password : 5
Numero massimo di giorni tra i cambi di password : 90
Giorni di preavviso prima della scadenza della password : 14
```

1.5. Ulteriori considerazioni sulla sicurezza

Molte applicazioni usano meccanismi di autenticazione alternativi che possono essere facilmente trascurati anche da esperti amministratori di sistema. Pertanto, è importante comprendere e controllare come avviene l'autenticazione degli utenti e come accedono ai servizi e alle applicazioni sul proprio server.

1.5.1. Accesso SSH per gli utenti disabilitati

Disattivando o bloccando l'account di un utente non impedisce che quest'ultimo riesca a effettuare l'accesso al server se precedentemente utilizzava una chiave pubblica RSA; saranno ancora in grado di ottenere l'accesso al server senza la necessità della password. Controllare sempre se nella directory home degli utenti sono presenti dei file che permettano questo tipo di autenticazione SSH, come per esempio `/home/nomeutente/.ssh/authorized_keys`.

Eliminare o rinominare la directory `.ssh/` nella home degli utenti per prevenire future autenticazioni SSH.

Assicurarsi di controllare qualsiasi connessione SSH stabilita dagli utenti disabilitati, dato che potrebbero esserci connessioni aperti in entrata o in uscita. Terminare tutte quelle che vengono trovate.

Limitare l'accesso SSH solo agli utenti che ne hanno il diritto. Per esempio, è possibile creare un gruppo chiamato «sshlogin» e aggiungere il nome del gruppo alla voce `AllowGroupsvarname> nel file /etc/ssh/sshd_config.`

```
AllowGroups sshlogin
```

Dopo aver aggiunto gli utenti con diritto di accesso SSH al gruppo «sshlogin», riavviare il server SSH.

```
sudo adduser NOME_UTENTE sshlogin
sudo service ssh restart
```

1.5.2. Autenticazione utenti su database esterno

La maggior parte delle reti aziendali richiedono un servizio di autenticazione e di controllo degli accessi centralizzato per tutte le risorse di sistema. Se il server è stato configurato per gestire l'autenticazione attraverso database esterni, assicurarsi di disabilitare gli account utente sia esternamente che internamente, in questo modo l'autenticazione locale di riserva non è più possibile.

2. Sicurezza della console

Come con qualsiasi altro sistema di protezione che viene usato per proteggere il proprio server, è molto difficile difendersi dai rischi imprevisti, causati da qualcuno con accesso fisico all'interno dell'ambiente di lavoro, come furti di dischi fissi, mancanza di corrente e via dicendo. Perciò, è necessario considerare la sicurezza della console come un componente della sicurezza totale del sistema. Una porta bloccata può fermare un malintenzionato o può almeno rallentare un ladro esperto, ed è quindi utile prendere delle precauzioni anche a livello della console.

Le seguenti istruzioni consentiranno di proteggere il proprio server da problemi che potrebbero portare serie conseguenze.

2.1. Disabilitare il Ctrl+Alt+Canc

Qualsiasi persona con accesso fisico alla tastiera può semplicemente premere **Ctrl**+**Alt**+**Canc** per riavviare il server senza eseguire l'accesso. Qualcuno può sempre scollegare la presa della corrente, ma per lo meno è da evitare l'uso di questa combinazione di tasti su un server in produzione. In questo modo un malintenzionato è costretto a utilizzare altre strategie per riavviare un server e consente di non riavviarlo accidentalmente.

- Per disabilitare il riavvio azionato dalla combinazione di tasti **Ctrl**+**Alt**+**Canc**, commentare la seguente riga nel file `/etc/init/control-alt-delete.conf`.

```
#exec shutdown -r now "Control-Alt-Delete pressed"
```

3. Firewall

3.1. Introduzione

Il kernel Linux include il sottosistema *Netfilter* usato per manipolare o decidere la sorte del traffico di rete diretto all'interno o attraverso un server. Tutte le moderne soluzioni firewall per Linux si basano su questo sistema di filtraggio dei pacchetti.

Il sistema di filtraggio dei pacchetti del kernel non è di grande utilità per gli amministratori senza un'interfaccia nello spazio utente per gestirlo. Questo è il compito di iptables. Quando un pacchetto raggiunge il proprio server, esso è gestito affidato al sottosistema Netfilter per l'accettazione, la manipolazione oppure il rifiuto secondo quanto stabilito da regole fornite al sottosistema dallo spazio utente attraverso iptables. Quindi, iptables è tutto ciò che è necessario per gestire il proprio firewall, a patto che si abbia la dimestichezza necessaria; sono comunque disponibili molte altre applicazioni per semplificare tale attività.

3.2. ufw - Firewall non complicato

L'applicazione predefinita in Ubuntu per la configurazione di un firewall è ufw. Sviluppato per semplificare la configurazione di iptables, ufw offre un modo semplice per creare un firewall basato su protocolli IPv4 e IPv6.

ufw, in modo predefinito, è inizialmente disabilitato. Dal manuale di ufw si legge:

«ufw is not intended to provide complete firewall functionality via its command interface, but instead provides an easy way to add or remove simple rules. It is currently mainly used for host-based firewalls (ufw non ha lo scopo di implementare tutte le funzionalità di un firewall tramite la sua interfaccia di comandi, ma invece cerca di facilitare l'aggiunta o la rimozione di semplici regole. È usato principalmente per dei firewall host-based)»

Seguono degli esempi sull'uso di ufw:

- Per prima cosa, è necessario abilitare ufw. In un terminale digitare:

```
sudo ufw enable
```

- Per aprire una porta (in questo caso la porta di SSH):

```
sudo ufw allow 22
```

- Le regole possono anche essere aggiunte usando un formato *a numeri*:

```
sudo ufw insert 1 allow 80
```

- Analogamente, per chiudere una porta aperta:

```
sudo ufw deny 22
```

- Per eliminare una regola, usare «delete» seguito dalla regola:

```
sudo ufw delete deny 22
```

- È anche possibile consentire l'accesso da host o da reti specifici a una porta. Il seguente esempio consente accesso SSH dall'host 192.168.0.2 a qualsiasi indirizzo IP su questo host:

```
sudo ufw allow proto tcp from 192.168.0.2 to any port 22
```

  Sostituire 192.168.0.2 con 192.168.0.0/24 per consentire accesso SSH da tutta la sotto-rete.

- Aggiungendo l'opzione *--dry-run* a un comando *ufw* è possibile visualizzare il risultato delle regole, ma senza applicarle. Per esempio, questo è quello che verrebbe applicato nel caso venisse aperta la porta HTTP:

```
sudo ufw --dry-run allow http
```

```
*filter
:ufw-user-input - [0:0]
:ufw-user-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
### RULES ###

### tuple ### allow tcp 80 0.0.0.0/0 any 0.0.0.0/0
-A ufw-user-input -p tcp --dport 80 -j ACCEPT

### END RULES ###
-A ufw-user-input -j RETURN
-A ufw-user-output -j RETURN
-A ufw-user-forward -j RETURN
-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix "[UFW LIMIT]: "
-A ufw-user-limit -j REJECT
-A ufw-user-limit-accept -j ACCEPT
COMMIT
Rules updated
```

- È possibile disabilitare ufw con il comando:

```
sudo ufw disable
```

- Per visualizzare lo stato del firewall usare:

```
sudo ufw status
```

- Per informazioni più dettagliate usare:

```
sudo ufw status verbose
```

- Per visualizzare il formato *a numeri*:

```
sudo ufw status numbered
```

Se la porta che si vuole aprire o chiudere è definita in `/etc/services`, è possibile usare il nome della porta al posto del numero. In questo esempio si sostituisce *22* con *ssh*.

Questa è una breve introduzione all'utilizzo di ufw. Per maggiori informazioni, consultare le pagine man di ufw.

3.2.1. Integrazione delle applicazioni con ufw

Le applicazioni che aprono delle porte possono includere un profilo ufw in cui vengono descritte le porte necessarie all'applicazione per funzionare correttamente. I profili vengono salvati in `/etc/ufw/applications.d` e possono essere modificati se le porte predefinite sono cambiate.

- Per visualizzare quali applicazioni hanno un profilo installato, in un terminale digitare:

```
sudo ufw app list
```

- Usare un profilo di un'applicazione è simile al consentire il traffico attraverso una porta:

```
sudo ufw allow Samba
```

- È disponibile anche una sintassi più estesa:

```
ufw allow from 192.168.0.0/24 to any app Samba
```

Sostituire *Samba* e *192.168.0.0/24* con il profilo dell'applicazione da usare e l'intervallo di indirizzi della propria rete.

Non è necessario specificare il *protocollo* per l'applicazione, dato che queste informazioni sono contenute nel profilo. Notare che il nome dell'*applicazione* sostituisce il numero della *porta*.

- Per visualizzare i dettagli riguardo quali porte, protocolli, ecc... sono definiti per un'applicazione, digitare:

```
sudo ufw app info Samba
```

Non tutte le applicazioni che richiedono l'apertura di una porta hanno un profilo ufw, ma se è stato creato un profilo per un'applicazione e lo si vuole includere nel pacchetto, segnalare un bug su Launchpad.

```
ubuntu-bug NOME_DEL_PACCHETTO
```

3.3. IP masquerading

Il compito dell'IP masquerading è di consentire a quei computer della rete forniti di indirizzi IP privati e non instradabili, di accedere a Internet tramite il computer che opera il masquerading. Il traffico che va dalla rete privata verso Internet deve essere manipolato per ottenere risposte che siano re-instradabili al computer che ne ha fatto richiesta. Per ottenere questo risultato, il kernel deve modificare l'indirizzo IP *sorgente* di ciascun pacchetto affinché tali risposte vengano re-instradate a esso invece che all'indirizzo IP privato che ha fatto la richiesta, procedura impossibile da eseguire su Internet. Linux fa uso del *tracciamento della connessione* (conntrack) per tenere traccia di quale connessione appartenga a quale computer e di conseguenza per re-instradare ciascun pacchetto di risposta. Il traffico in uscita dalla rete privata viene quindi «mascherato» per simulare l'uscita dalla macchina gateway Ubuntu. Nella documentazione Microsoft questo processo è indicato come condivisione delle connessioni internet (Internet Connection Sharing).

3.3.1. Masquerading con ufw

L'IP masquerading può essere ottenuto utilizzando regole ufw personalizzate. Questo è possibile dato che il backend attuale per ufw è iptables-restore con i file delle regole posizionati in `/etc/ufw/*.rules`. Questi file possono essere usati per aggiungere vecchie regole di iptables usate senza ufw e regole maggiormente legate al gateway o al bridge.

Le regole sono divise in due file diversi, regole da eseguire prima delle regole a riga di comando di ufw e regole da eseguire dopo ufw.

- Per prima cosa, è necessario abilitare l'inoltro dei pacchetti modificando due file di configurazione. In `/etc/default/ufw` modificare *DEFAULT_FORWARD_POLICY* in «ACCEPT»:

  ```
  DEFAULT_FORWARD_POLICY="ACCEPT"
  ```

  Quindi modificare il file `/etc/ufw/sysctl.conf` de-commentando:

  ```
  net/ipv4/ip_forward=1
  ```

  Similmente, per abilitare l'inoltro con IPv6 de-commentare:

  ```
  net/ipv6/conf/default/forwarding=1
  ```

- Ora verranno aggiunte delle regole al file `/etc/ufw/before.rules`. Le regole predefinite configurano solamente la tabella *filter* e per abilitare il masquerading è necessario configurare la tabella *nat*. Aggiungere all'inizio del file, subito dopo i commenti dell'intestazione, quanto segue:

  ```
  # regole tabella nat
  *nat
  :POSTROUTING ACCEPT [0:0]
  ```

```
# Inoltro traffico da eth1 attraverso eth0
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

# non cancellare la riga 'COMMIT' o queste tabelle di regole non saranno elaborate
COMMIT
```

I commenti non sono necessari, ma è buona pratica documentare le proprie configurazioni. Inoltre, quando si modificano i file *rules* in `/etc/ufw`, assicurarsi che queste righe siano sempre le ultime in ogni tabella modificata:

```
# non eliminare la riga 'COMMIT' o queste tabelle di regole non saranno elaborate
COMMIT
```

Per ogni *tabella* è necessario un *COMMIT*. In questi esempi sono mostrate solamente le tabelle *nat* e *filter*, ma è possibile aggiungere regole per le tabelle *raw* e *mangle*.

Nell'esempio precedente, sostituire *eth0*, *eth1* e *192.168.0.0/24* con le interfacce appropriate e con l'intervallo di indirizzi corretto.

- Infine, disattivare e riattivare ufw per applicare le modifiche:

```
sudo ufw disable && sudo ufw enable
```

L'IP masquerading ora dovrebbe essere abilitato. È possibile aggiungere regole FORWARD aggiuntive al file `/etc/ufw/before.rules`. È utile che queste regole addizionali vengano aggiunte alla catena *ufw-before-forward*.

3.3.2. Masquerading con iptables

È possibile usare iptables per abilitare Masquerading.

- Similmente a ufw, il primo passo per abilitare l'inoltro di pacchetti con IPv4 è quello di modificare il file `/etc/sysctl.conf` e de-commentare la seguente riga:

```
net.ipv4.ip_forward=1
```

Per abilitare l'inoltro con IPv6, de-commetare:

```
net.ipv6.conf.default.forwarding=1
```

- Quindi, eseguire il comando sysctl per abilitare le nuove impostazioni nel file di configurazione:

```
sudo sysctl -p
```

- L'IP masquerading può essere ottenuto con una sola regola di iptables, che può cambiare leggermente in base alla configurazione della propria rete:

```
sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
```

Il comando precedente assume che lo spazio di indirizzi privato sia 192.168.0.0/16 e che il dispositivo collegato a Internet sia ppp0. La sintassi del comando è la seguente:

- -t nat: regola viene inserita nella tabella nat
- -A POSTROUTING: la regola viene accodata (-A) alla catena POSTROUTING
- -s 192.168.0.0/16: la regola si applica al traffico originato dallo spazio di indirizzi specificato
- -o ppp0: la regola si applica al traffico instradato attraverso l'interfaccia di rete specificata
- -j MASQUERADE: il traffico che soddisfa questa regola viene «saltato» (-j sta per jump) alla destinazione MASQUERADE per essere manipolato come descritto in precedenza

- Inoltre, ogni catena nella tabella «filter» (la tabella predefinita e dove avvengono la maggior parte dei filtri sui pacchetti) ha una *politica* predefinita di ACCEPT, ma se si sta creando un firewall in aggiunta a un dispositivo gateway, è possibile aver impostato le politiche DROP e REJECT, nel cui caso il traffico «masqueraded» deve essere consentito attraverso la catena FORWARD affinché la regola precedente possa funzionare:

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.0.0/16 -m state \
--state ESTABLISHED,RELATED -i ppp0 -j ACCEPT
```

  I precedenti comandi consentiranno a tutte le connessioni della propria rete locale accesso a Internet e a tutto il traffico relativo a queste connessioni di ritornare ai computer che lo hanno originato.

- Per fare in modo che il masquerading sia abilitato al riavvio, modificare il file `/etc/rc.local` e aggiungere qualsiasi dei comandi utilizzati precedentemente. Per esempio, aggiungere il primo comando senza filtro:

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
```

3.4. Registri

I registri del firewall sono molto utili per riconoscere gli attacchi, migliorare le regole del firewall e per verificare attività inusuali nella propria rete. È necessario includere regole di registrazione per fare in modo che vengano eseguite le registrazioni e queste devono essere inserite prima di qualsiasi regola terminante applicabile (un regola con un obiettivo che decide il destino di un pacchetto, come ACCEPT, DROP o REJECT).

Se si sta usando ufw è possibile attivare la registrazione con il seguente comando:

```
sudo ufw logging on
```

Per disabilitare la registrazione in ufw, sostituire, nel comando precedente, *on* con *off*.

Se è in uso iptables al posto di ufw, digitare:

```
sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 \
-j LOG --log-prefix "NEW_HTTP_CONN: "
```

Una richiesta sulla porta 80 dal computer locale genererebbe, in dmesg, una traccia simile a questa (unica riga divisa in 3 per adattarla al formato di questo documento):

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00
 SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=58288 DF PROTO=TCP
 SPT=53981 DPT=80 WINDOW=32767 RES=0x00 SYN URGP=0
```

Il registro precedente appare anche in `/var/log/messages`, `/var/log/syslog` e `/var/log/kern.log`. Questo comportamento può essere cambiato, modificando in modo appropriato il file `/etc/syslog.conf` oppure installando e configurando ulogd e facendo uso della destinazione ULOG al posto di LOG. Il demone ulogd è un server nello spazio utente in ascolto per le istruzioni di registro del kernel specifiche dei firewall; è possibile salvare i registri su qualsiasi file o perfino in un database come PostgreSQL o MySQL. Per dare un significato ai registri del firewall è possibile utilizzare delle applicazioni di analisi dei registri come logwatch, fwanalog, fwlogwatch o lire.

3.5. Altri strumenti

Esistono diversi strumenti per «costruire» un firewall completo senza alcuna conoscenza di iptables. Per chi preferisce un'interfaccia grafica:

- *fwbuilder*[1] è molto potente e ha un aspetto che può risultare familiare agli amministratori che hanno utilizzato un firewall commerciale come Checkpoint FireWall-1.

Per chi preferisce uno strumento a riga di comando con file di configurazione in semplice testo:

- *Shorewall*[2] è una soluzione molto potente per configurare un firewall di livello avanzato per qualsiasi rete.

3.6. Riferimenti

- La pagina relativa a *Ubuntu Firewall*[3] della documentazione contiene informazioni sullo sviluppo di ufw.
- Inoltre, la pagina del manuale ufw contiene alcune informazioni molto utili: **man ufw**.
- Per ulteriori informazioni sull'utilizzo di iptables, consultare *packet-filtering-HOWTO*[4].
- Il *nat-HOWTO*[5] contiene ulteriori dettagli sul masquerading.
- La pagine della documentazione della comunità *IPTables HowTo*[6] è una grande risorsa.

[1] http://www.fwbuilder.org/
[2] http://www.shorewall.net/
[3] https://wiki.ubuntu.com/UncomplicatedFirewall
[4] http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html
[5] http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html
[6] https://help.ubuntu.com/community/IptablesHowTo

4. AppArmor

AppArmor è un'implementazione del «Linux Security Module» per il controllo degli accessi vincolante basato sul nome. AppArmor racchiude individualmente i programmi in un insieme di file e capacità posix 1003.1e draft.

AppArmor è installato e caricato in modo predefinito e utilizza i *profili* di un'applicazione per determinare quali file e permessi siano necessari all'applicazione. Alcuni pacchetti installano i propri profili e ulteriori profili possono essere trovati nel pacchetto apparmor-profiles.

Per installare il pacchetto apparmor-profiles, in un terminale digitare:

```
sudo apt-get install apparmor-profiles
```

I profili di AppArmor dispongono di due modalità di esecuzione:

- Apprendimento (complaining/learning): le violazioni del profilo sono consentite e vengono registrate. Utile per verificare e sviluppare nuovi profili.
- Esecutiva (enforced/confined): obbliga a rispettare la politica del profilo e registra le violazioni.

4.1. Utilizzare AppArmor

Il pacchetto apparmor-utils contiene utilità a riga di comando che è possibile usare per modificare la modalità di esecuzione di AppArmor, trovare lo stato di un profilo, creare nuovi profili, ecc...

- apparmor_status è utilizzata per visualizzare lo stato attuale dei profili AppArmor.

  ```
  sudo apparmor_status
  ```

- aa-complain posiziona un profilo nella modalità *apprendimento*.

  ```
  sudo aa-complain /percorso/al/binario
  ```

- aa-enforce posiziona un profilo nella modalità *esecutiva*.

  ```
  sudo aa-enforce /percorso/al/bianrio
  ```

- Nella directory `/etc/apparmor.d` sono archiviati tutti i profili di AppArmor ed è possibile, da qui, modificare la *modalità* di tutti i profili.

  Usare il seguente comando per impostare tutti i profili nella modalità apprendimento:

  ```
  sudo aa-complain /etc/apparmor.d/*
  ```

  Per impostare tutti i profili nella modalità esecutiva:

  ```
  sudo aa-enforce /etc/apparmor.d/*
  ```

- apparmor_parser è utilizzata per caricare un profilo all'interno del kernel. Può essere usata anche per ricaricare profili attraverso l'opzione *-r*. Per caricare un profilo:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

  Per ricaricare un profilo:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -r
```

- `service apparmor` can be used to *reload* all profiles:

```
sudo service apparmor reload
```

- La directory `/etc/apparmor.d/disable` può essere usata con l'opzione apparmor_parser -R per *disabilitare* un profilo.

```
sudo ln -s /etc/apparmor.d/profile.name /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/profile.name
```

  Per *riabilitare* un profilo disabilitato, rimuovere il collegamento simbolico al profilo in `/etc/apparmor.d/disable/`, quindi caricare il profilo usando l'opzione *-a*.

```
sudo rm /etc/apparmor.d/disable/profile.name
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

- È possibile disabilitare AppArmor e scaricare il modulo del kernel attraverso i seguenti comandi:

```
sudo service apparmor stop
sudo update-rc.d -f apparmor remove
```

- Per riabilitare AppArmor:

```
sudo service apparmor start
sudo update-rc.d apparmor defaults
```

Sostituire *profile.name* con il nome del profilo da modificare e sostituire anche `/percorso/eseguibile/` con il percorso all'eseguibile. Per esempio, per il comando ping, usare `/bin/ping`

4.2. Profili

I profili di AppArmor sono dei semplici file di testo posizionati in `/etc/apparmor.d/`. Questi file vengono nominati con il percorso completo all'eseguibile del profilo, sostituendo «/» con «.». Per esempio, `/etc/apparmor.d/bin.ping` è il profilo AppArmor del comando `/bin/ping`.

Esistono due principali tipologie di regole usate nei profili:

- *Voci di percorso*: specificano a quali file nel file system un'applicazione può accedere.

- *Voci di capacità*: determinano quali privilegi un processo può utilizzare.

Per un esempio, consultare `/etc/apparmor.d/bin.ping`:

```
#include <tunables/global>
/bin/ping flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/consoles>
  #include <abstractions/nameservice>

  capability net_raw,
  capability setuid,
  network inet raw,

  /bin/ping mixr,
  /etc/modules.conf r,
}
```

- *#include <tunables/global>*: asserzioni di inclusione da altri file. Consente di usare un file comune con le asserzioni di inclusione per molteplici applicazioni.
- */bin/ping flags=(complain)*: percorso al programma con profilo, impostandone la modalità ad *apprendimento*.
- *capability net_raw,*: consente all'applicazione di accedere alla capacità CAP_NET_RAW Posix.1e.
- */bin/ping mixr,*: consente all'applicazione accesso in lettura e in esecuzione al file.

Dopo aver modificato un profilo, è necessario ricaricarlo. Per maggiori informazioni, consultare *Sezione 4.1, «Utilizzare AppArmor» [168]*.

4.2.1. Creare un profilo

- *Progettare un piano di verifica*: cercare di pensare a come l'applicazione dovrebbe essere eseguita. Il piano di verifica dovrebbe essere diviso in tanti piccoli casi d'uso, ognuno dei quali dovrebbe avere una breve descrizione e un elenco dei passi da compiere.

  Alcuni casi standard da verificare sono:

  - Avvio del programma.
  - Arresto del programma.
  - Ricaricamento del programma.
  - Verifica di tutti i comandi supportati dallo script init.
- *Generare il nuovo profilo*: usare aa-genprof per generare un nuovo profilo. Da un terminale:

  ```
  sudo aa-genprof eseguibile
  ```

  Per esempio:

```
sudo aa-genprof slapd
```

- Affinché il proprio nuovo profilo venga incluso nel pacchetto apparmor-profiles, segnalare un bug su *Launchpad* riguardo il pacchetto *AppArmor*[7]:
  - Includere la pianificazione e le casistiche del test.
  - Allegare il nuovo profilo al bug.

4.2.2. Aggiornare i profili

Quando il programma si comporta stranamente, messaggi di audit vengono inviati ai file di registro. Il programma aa-logprof può essere usato per analizzare i file di registro per i messaggi di audit di AppArmor, per controllarli e per aggiornare i profili. Da un terminale:

```
sudo aa-logprof
```

4.3. Riferimenti

- Per le opzioni avanzate di configurazione, consultare la *AppArmor Administration Guide*[8]
- Per maggiori informazioni su come usare AppArmor con altri rilasci di Ubuntu, consultare la *documentazione della comunità italiana*[9].
- La pagina *OpenSUSE AppArmor*[10] contiene un'altra introduzione ad AppArmor.
- Un buon posto per chiedere assistenza riguardo AppArmor, e per partecipare nella comunità di Ubuntu Server, è il canale IRC *#ubuntu-server* su *freenode*[11].

---

7 https://bugs.launchpad.net/ubuntu/+source/apparmor/+filebug
8 http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/index.html?page=/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html
9 http://wiki.ubuntu-it.org/Sicurezza/AppArmor
10 http://en.opensuse.org/SDB:AppArmor_geeks
11 http://freenode.net

5. Certificati

Una delle più comuni forme di crittografia odierna è la crittografia a *chiave pubblica*. Questo tipo di crittografia utilizza una *chiave pubblica* e una *chiave privata*. Il sistema funziona *cifrando* le informazioni usando la chiave pubblica che possono solo essere *decifrate* con la chiave privata.

L'utilizzo più comune della crittografia a chiave pubblica è nella cifratura del traffico delle applicazioni attraverso una connessione SSL (Secure Socket Layer) o TLS (Transport Layer Security), per esempio configurando Apache affinché fornisca *HTTPS*, il protocollo HTTP via SSL. Questo consente di cifrare il traffico utilizzando un protocollo che non fornisce nativamente una cifratura.

Un *certificato* è un metodo di distribuzione di una *chiave pubblica* e di altre informazioni riguardo un server e l'organizzazione che ne è responsabile. I certificati possono essere firmati digitalmente a un'*Autorità di Certificazione* o CA. Una CA è un'entità fidata che conferma la veridicità delle informazioni contenute nel certificato.

5.1. Tipologie dei certificati

Per configurare un server sicuro affinché usi la crittografia a chiave pubblica, nella maggior parte dei casi, è necessario inviare la richiesta del certificato (compresa la chiave pubblica), una prova di esistenza della propria società e il pagamento a una CA. La CA verifica la richiesta e la propria identità e quindi invia un certificato per il proprio server. In alternativa, è possibile creare il proprio certificato *auto-firmato*.

I certificati auto-firmati non dovrebbero essere usati in ambienti di produzione.

Continuando l'esempio di HTTPS, un certificato CA firmato dispone di caratteristiche che un certificato auto-firmato non ha:

- I browser, solitamente, riconoscono automaticamente il certificato e consentono l'attivazione di una connessione sicura senza chiedere nulla all'utente.
- Quando una CA emette un certificato, garantisce l'identità dell'organizzazione che fornisce la pagina web al browser.

La maggior parte dei browser web, e dei computer che supportano SSL, dispongono di un elenco di CA i cui certificati sono accettati automaticamente. Se un browser incontra un certificato la cui CA non è presente nell'elenco, il browser chiede all'utente di accettare o rifiutare la connessione. Inoltre, altre applicazioni possono generare un messaggio di errore quando viene usato un certificato auto-firmato.

Il processo per ottenere un certificato da una CA è molto semplice. Un piccolo promemoria:

1. Creare un coppia di chiavi pubblica e privata.
2. Creare una richiesta per un certificato basato su chiave pubblica. La richiesta del certificato contiene informazioni riguardo il server a la società che lo ospita.

3. Inviare la richiesta, con una fotocopia di un documento di identità, a una CA. Non è possibile consigliare quale autorità di certificazione scegliere. La decisione potrebbe essere basata su esperienze passate, esperienze di amici o colleghi o per un fattore economico.

   Una volta scelta la CA, è necessario seguire le istruzioni fornite dal CA per ottenere il certificato.
4. Una volta che la CA ha verificato l'identità del richiedente, invierà un certificato digitale.
5. Installare questo certificato sul proprio server sicuro e configurare le applicazioni appropriate affinché usino il certificato.

5.2. Generare una CSR (Certificate Signing Request)

Sia che si stia ottenendo un certificato da una CA sia che si auto-firmi il proprio, il primo passo consiste nel generare una chiave di cifratura.

Se il certificato verrà usato da servizi come Apache, Postfix, Dovect, ecc..., è solitamente indicato usare una chiave priva di passphrase.

Questa sezione indica come generare una chiave dotata di passphrase e una priva di passphrase. La chiave priva di passphrase verrà impiegata per generare un certificato che può essere usato da diversi servizi.

Avere in esecuzione i servizi senza una passphrase è conveniente poiché non vi è la necessità di digitare la passphrase a ogni avvio del servizio, ma non è molto sicuro in quanto se la chiave viene compromessa, verrà compromesso anche il server.

Per generare le *chiavi* per la CSR (Certificate Signing Request), eseguire in un terminale il seguente comando:

```
openssl genrsa -des3 -out server.key 2048
```

```
Generating RSA private key, 2048 bit long modulus
..........................++++++
.......++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

È ora necessario inserire una passphrase. Per una maggiore sicurezza, dovrebbe contenere almeno 8 caratteri. La lunghezza minima con l'opzione «-des3» è di 4 caratteri. Dovrebbe includere numeri o segni di punteggiatura e non dovrebbe essere una parola reperibile in un vocabolario. Ricordarsi che una passphrase differenzia tra minuscole e maiuscole.

Digitare nuovamente la passphrase per la verifica. Una volta digitata correttamente, la chiave per il server viene generata e archiviata nel file `server.key`.

Creare la chiave insicura, quella priva di passphrase, e scambiare i nomi delle chiavi:

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

La chiave insicura è ora chiamata `server.key` ed è possibile usare questo file per generare la CSR senza passphrase.

Per creare il CSR, eseguire il seguente comando:

```
openssl req -new -key server.key -out server.csr
```

Viene chiesto di inserire la passphrase; se viene inserita la passphrase corretta, viene chiesto di inserire il nome della società, nome del sito, email ecc... Una volta inseriti tutti questi dettagli, la CSR viene creata e archiviata nel file `server.csr` file.

È ora possibile inviare il file della CSR alla CA che lo utilizzerà per creare il certificato finale. È comunque possibile creare un certificato auto-firmato utilizzando questa CSR.

5.3. Creare un certificato auto-firmato

Per creare un certificato auto-firmato, eseguire da un terminale il seguente comando:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Il comando precedente chiederà la passphrase. Una volta digitata correttamente, il certificato viene creato e sarà disponibile nel file `server.crt`.

Se il server deve essere utilizzato in ambito commerciale, è necessario un certificato emesso da una CA. Non è raccomandato utilizzare un certificato auto-firmato.

5.4. Installare il certificato

È possibile installare il file `server.key` e quello del certificato `server.crt`, o il file del certificato fornito dalla CA, eseguendo, in un terminale, i seguenti comandi:

```
sudo cp server.crt /etc/ssl/certs
sudo cp server.key /etc/ssl/private
```

Ora basta configurare le applicazioni che possono usare la crittografia a chiave pubblica affinché utilizzino i file del *certificato* e della *chiave*. Per esempio, Apache può fornire HTTPS, Dovecot può fornire IMAPS e POP3S ecc...

5.5. Autorità di Certificazione

Se i servizi all'interno della propria rete richiedono più di un certificato auto-firmato, potrebbe essere utile impostare una *Autorità di Certificazione* personale. Usando certificati firmati dalla propria CA,

consente ai vari servizi che usano tali certificati di fidarsi di altri servizi che fanno uso di certificati emessi dalla stessa CA.

1. Per prima cosa, creare le directory che conterranno il certificato della CA e i file relativi

```
sudo mkdir /etc/ssl/CA
sudo mkdir /etc/ssl/newcerts
```

2. La CA necessita di alcuni altri file per funzionare correttamente: uno per tenere traccia dell'ultimo numero seriale usato (ogni certificato deve avere un numero univoco) e l'altro per registrare quali certificati sono stati emessi:

```
sudo sh -c "echo '01' > /etc/ssl/CA/serial"
sudo touch /etc/ssl/CA/index.txt
```

3. Il terzo file è il file di configurazione della CA. Benché non strettamente necessario, è molto utile quando vengono emessi certificati multipli. Aprire il file `/etc/ssl/openssl.cnf` e nella sezione *[CA_default]* modificare:

```
dir             = /etc/ssl/             # Dove viene salvato tutto
database        = $dir/CA/index.txt     # File indice del database
certificate     = $dir/certs/cacert.pem # Il certificato della CA
serial          = $dir/CA/serial        # Il numero seriale corrente
private_key     = $dir/private/cakey.pem# La chiave privata
```

4. Creare il certificato auto-firmato principale:

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

   Viene chiesto di inserire i dettagli del certificato.

5. Installare il certificato principale e la chiave:

```
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

6. È ora possibile firmare i certificati. La prima cosa necessaria è una CSR (Certificate Signing Request), consultare *Sezione 5.2, «Generare una CSR (Certificate Signing Request)» [173]*. Una volta ottenuta, digitare quanto segue per generare un certificato firmato dalla CA:

```
sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

   Inserita la passoword della chiave CA, viene chiesto di firmare il certificato e di generare quello nuovo. Dovrebbe quindi essere visibile l'output della generazione del certificato stesso.

7. Dovrebbe essere presente un nuovo file, `/etc/ssl/newcerts/01.pem`, contenente il medesimo output. Copiare tutto ciò che è compreso tra -----*BEGIN CERTIFICATE*----- e ----*END CERTIFICATE*----- e incollarlo in un file chiamato come il nome host del server in cui verrà installato; per esempio: `mail.example.com.crt` è un nome descrittivo appropriato.

Tutti i certificati successivi saranno chiamati `02.pem`, `03.pem`, ecc...

Sostituire *mail.example.com.crt* con un nome descrittivo appropriato al proprio caso.

8. In fine, copiare il nuovo certificato nell'host e configurare le applicazioni al suo uso. La posizione predefinita per l'installazione dei certificati è `/etc/ssl/certs`, consentendo così a molteplici servizi di usare lo stesso certificato senza complicare inutilmente i permessi.

   Per le applicazioni che possono essere configurate all'uso di un certificato di una CA, è necessario copiare il file `/etc/ssl/certs/cacert.pem` nella directory `/etc/ssl/certs/` di ogni server.

5.6. Riferimenti

- Per ulteriori informazioni sull'utilizzo della crittografia, consultare lo *SSL Certificates HOWTO*[12].
- La pagina Wikipedia *HTTPS*[13] dispone di ulteriori informazioni riguardo HTTPS.
- Per maggiori informazioni riguardo *OpenSSL*, consultare il *sito web di OpenSSL*[14].
- Inoltre, il libro *Network Security with OpenSSL*[15] di O'Reilly è un ottimo punto di riferimento.

[12] http://tldp.org/HOWTO/SSL-Certificates-HOWTO/index.html
[13] http://it.wikipedia.org/wiki/HTTPS
[14] http://www.openssl.org/
[15] http://oreilly.com/catalog/9780596002701/

6. eCryptfs

eCryptfs è un file system crittografico POSIX-conforme per Linux. Disponendosi al di sopra del livello del file system normale, *eCryptfs* è in grado di proteggere i file indipendentemente dal file system sottostante, dal tipo di partizione, ecc...

Durante la fase di installazione è disponibile un'opzione per cifrare l'intera partizione `/home` in grado di configurare tutto il necessario per cifrare e montare la partizione.

Questa sezione spiega come configurare `/srv` per cifrarla con *eCryptfs*.

6.1. Usare eCryptfs

Per prima cosa, installare i pacchetti necessari. In un terminale digitare:

```
sudo apt-get install ecryptfs-utils
```

Montare la partizione da cifrare:

```
sudo mount -t ecryptfs /srv /srv
```

Vengono chiesti alcuni dettagli su come ecryptfs dovrebbe cifrare i dati.

Per verificare che i file in `/srv` siano veramente cifrati, copiare la directory `/etc/default` in `/srv`:

```
sudo cp -r /etc/default /srv
```

Smontare `/srv` e cercare di visualizzare un file:

```
sudo umount /srv
cat /srv/default/cron
```

Montare `/srv` utilizzando ecryptfs per poter visualizzare nuovamente i dati.

6.2. Montare automaticamente le partizioni cifrate

È possibile montare un file system ecryptfs in diversi modi all'avvio. Questo esempio fa uso di un file `/root/.ecryptfsrc` contenente le opzioni di mount e un file, salvato su una chiave USB, contenente la passphrase.

Creare il file `/root/.ecryptfsrc` contenente:

```
key=passphrase:passphrase_passwd_file=/mnt/usb/passwd_file.txt
ecryptfs_sig=5826dd62cf81c615
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
```

```
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

Modificare il campo *ecryptfs_sig* con la firma presente in `/root/.ecryptfs/sig-cache.txt`.

Creare il file `/mnt/usb/passwd_file.txt` per la passphrase:

```
passphrase_passwd=[secrets]
```

Aggiungere quanto necessario in `/etc/fstab`:

```
/dev/sdb1       /mnt/usb        ext3    ro      0 0
/srv /srv ecryptfs defaults 0 0
```

Assicurarsi che il dispositivo USB venga montato prima della partizione cifrata.

Infine, riavviare il computer e `/srv` dovrebbe essere montata tramite *eCryptfs*.

6.3. Altre utilità

Il pacchetto ecryptfs-utils contiene diverse utilità:

- *ecryptfs-setup-private*: crea una directory `~/Private` per contenere informazioni cifrate. Questa utilità può essere eseguita da utenti senza alcun tipo di privilegio all'interno del sistema per creare una piccola zona privata dove salvare dati.
- *ecryptfs-mount-private* e *ecryptfs-umount-private*: monta e smonta la directory `~/Private` degli utenti.
- *ecryptfs-add-passphrase*: aggiunge una nuova passphrase al portachiavi.
- *ecryptfs-manager*: gestisce gli oggetti eCryptfs come le chiavi.
- *ecryptfs-stat* consente di visualizzare le meta informazioni di ecryptfs relative a un file.

6.4. Riferimenti

- Per ulteriori informazioni su *eCryptfs*, consultare la pagina di Launchpad di .[16]
- In *Linux Journal*[17] c'è un articolo su *eCryptfs*.
- Also, for more ecryptfs options see the *ecryptfs man page*[18].
- La pagina della *documentazione della comunità su eCryptfs*[19] contiene ulteriori dettagli.

16 https://launchpad.net/ecryptfs
17 http://www.linuxjournal.com/article/9400
18 http://manpages.ubuntu.com/manpages/quantal/en/man7/ecryptfs.7.html
19 https://help.ubuntu.com/community/eCryptfs

Capitolo 10. Monitoraggio

1. Panoramica

Il monitoraggio di server e servizi essenziali è un aspetto importante dell'amministrazione di sistema. La maggior parte dei servizi di rete vengono monitorati per controllarne prestazioni, disponibilità oppure entrambi. Questa sezione descrive l'installazione e la configurazione di Nagios per il monitoraggio mirato alla disponibilità dei servizi e di Munin per il monitoraggio delle prestazioni.

Gli esempi in questa sezione utilizzano due server con nome host *server01* e *server02*. Il server chiamato *server01* viene configurato con Nagios per monitorare i servizi sul server stesso e su *server02*. Inoltre, viene configurato anche munin per raccogliere informazioni dalla rete. Utilizzando il pacchetto munin-node, *server02* viene configurato per inviare informazioni a *server01*.

Questi semplici esempi dovrebbero permettere di monitorare server aggiuntivi e servizi all'interno della rete.

2. Nagios

2.1. Installazione

Per prima cosa, su *server01* installare il pacchetto nagios. In un terminale digitare:

```
sudo apt-get install nagios3 nagios-nrpe-plugin
```

Viene chiesto di inserire una password per l'utente *nagiosadmin*. Le credenziali vengono salvate nel file `/etc/nagios3/htpasswd.users`. Per modificare la password dell'utente *nagiosadmin* o per aggiungere altri utenti, usare il comando htpasswd, parte del pacchetto apache2-utils.

Per esempio, per modificare la password dell'utente *nagiosadmin* digitare:

```
sudo htpasswd /etc/nagios3/htpasswd.users nagiosadmin
```

Per aggiungere un utente:

```
sudo htpasswd /etc/nagios3/htpasswd.users steve
```

Su *server02* installare il pacchetto nagios-nrpe-server. Da un terminale su server02 inserire:

```
sudo apt-get install nagios-nrpe-server
```

NRPE consente di eseguire controlli locali sugli host remoti. Esistono anche altri metodi per eseguire questo attraverso l'uso di altri plugin o controlli di Nagios.

2.2. Panoramica della configurazione

Esistono diverse directory contenenti file di configurazione e di controllo di Nagios.

- `/etc/nagios3`: contiene i file di configurazione per le operazioni del demone nagios, i file CGI, host, ecc...
- `/etc/nagios-plugins`: contiene i file di configurazione per i controlli del servizio.
- `/etc/nagios`: sull'host remoto contiene i file di configurazione di nagios-nrpe-server.
- `/usr/lib/nagios/plugins/`: contiene i file binari dei controlli. Per visualizzare le opzioni di un controllo, usare l'opzione -*h*.

  Per esempio: **/usr/lib/nagios/plugins/check_dhcp -h**

Esistono moltissimi controlli che è possibile eseguire tramite Nagios su un qualsiasi host. In questo esempio Nagios viene configurato per controlla lo spazio su disco, DNS e un gruppo di host MySQL. Il controllo DNS avviene su *server02* e il gruppo di host MySQL include sia *server01* che *server02*.

Consultare *Sezione 1, «HTTPD - Server web Apache2» [188]* per informazioni su Apache, *Capitolo 8, DNS (Domain Name Service) [140]* su DNS e *Sezione 1, «MySQL» [207]* su MySQL.

Inoltre, vi sono alcuni termini che una volta descritti, aiuteranno a rendere più semplice la comprensione di Nagios:

- *Host*: un server, una workstation o un dispositivo di rete che viene monitorato.
- *Gruppo di host*: un gruppo di host simili. Per esempio potrebbe essere possibile raggruppare tutti i server web, i server di file, ecc...
- *Servizio*: il servizio che viene monitorato sull'host come HTTP, DNS, FTP, ecc...
- *Gruppo di servizi*: consente di raggruppare servizi simili. Utile, per esempio, per raggruppare più servizi HTTP.
- *Contatto*: una persona da notificare quando si verifica un evento. Nagios può essere configurato per inviare email, SMS, ecc...

Come impostazione predefinita, Nagios è configurato per controllare HTTP, spazio su disco, SSH, gli utenti attuali, i processi e il carico sul *localhost*. Inoltre, è in grado di controllare attraverso il comando ping il *gateway*.

Installazioni di Nagios di grosse dimensioni possono essere complesse da configurare ed è quindi utile partire con una configurazione piccola, uno o due host, prima di aumentare le dimensioni.

2.3. Configurazione

1. Per prima cosa, creare un file di configurazione *host* per *server02*; se non diversamente specificato, eseguire tutti questi comandi su *server01*. In un terminale digitare:

```
sudo cp /etc/nagios3/conf.d/localhost_nagios2.cfg \ /etc/nagios3/conf.d/server02.cfg
```

Nei comandi precedenti e in quelli che seguono, sostituire *«server01»*, *«server02»*, *172.18.100.100* e *172.18.100.101* con i nomi host e gli indirizzi IP dei propri server.

2. Modificare il file `/etc/nagios3/conf.d/server02.cfg`:

```
define host{
        use generic-host ; Name of host template to use
        host_name server02
        alias Server 02
        address 172.18.100.101
}

# check DNS service.
define service {
        use generic-service
        host_name server02
        service_description DNS
```

```
        check_command check_dns!172.18.100.101
}
```

3. Riavviare il demone nagios per abilitare la nuova configurazione:

```
sudo service nagios3 restart
```

- 1. Aggiungere una definizione di servizio per il controllo MySQL aggiungendo quanto segue al file `/etc/nagios3/conf.d/services_nagios2.cfg`:

```
# check MySQL servers.
define service {
        hostgroup_name mysql-servers
        service_description MySQL
        check_command check_mysql_cmdlinecred!nagios!secret!$HOSTADDRESS
        use generic-service
        notification_interval 0 ; set > 0 if you want to be renotified
}
```

2. È necessario definire un gruppo di host *mysql-servers*; modificare il file `/etc/nagios3/conf.d/hostgroups_nagios2.cfg` aggiungendovi:

```
# MySQL hostgroup.
define hostgroup {
        hostgroup_name  mysql-servers
                alias           MySQL servers
                members         localhost, server02
        }
```

3. Il controllo di Nagios necessita di autenticarsi con MySQL. Per aggiungere un utente *nagios* a MySQL inserire:

```
mysql -u root -p -e "create user nagios identified by 'secret';"
```

È necessario aggiungere l'utente *nagios* a tutti gli host del gruppo *mysql-servers*.

4. Riavviare nagios per iniziare il controllo dei server MySQL.

```
sudo service nagios3 restart
```

- 1. Infine configurare NRPE affinché controlli lo spazio su disco su *server02*.

  Sul *server01* aggiungere il controllo del servizio al file `/etc/nagios3/conf.d/server02.cfg`:

```
# NRPE disk check.
define service {
        use generic-service
        host_name server02
        service_description nrpe-disk
```

```
        check_command check_nrpe_1arg!check_all_disks!172.18.100.101
}
```

2. Su *server02* modificare il file `/etc/nagios/nrpe.cfg`:

   ```
   allowed_hosts=172.18.100.100
   ```

   E nella sezione dove sono definiti i comandi, aggiungere:

   ```
   command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
   ```

3. Infine, riavviare nagios-nrpe-server:

   ```
   sudo service nagios-nrpe-server restart
   ```

4. Riavviare, su *server01*, nagios:

   ```
   sudo service nagios3 restart
   ```

Dovrebbe essere possibile visualizzare l'host e i controlli nei file CGI di Nagios. Per accedere a questi file, in un browser web inserire l'indirizzo http://server01/nagios3. Vengono richiesti password e nome utente dell'utente *nagiosadmin*.

2.4. Riferimenti

Questa sezione ha fornito una panoramica preliminare delle caratteristiche di Nagios, i pacchetti nagios-plugins-extra e nagios-snmp-plugins contengono molti altri controlli.

- Per maggiori informazioni, consultare il sito web di *Nagios*[1].
- In particolare, consultare la *documentazione in rete*[2].
- Sono disponibili anche molti *libri*[3] riguardo Nagios e il monitoraggio di rete:
- Maggiori informazioni possono essere trovate nella *documentazione online della comunità su Nagios*[4].

[1] http://www.nagios.org/
[2] http://nagios.sourceforge.net/docs/3_0/
[3] http://www.nagios.org/propaganda/books/
[4] https://help.ubuntu.com/community/Nagios

3. Munin

3.1. Installazione

Prima di installare Munin su *server01*, è necessario installare apache2. La configurazione predefinita è sufficiente per poter eseguire un server munin. Per maggiori informazioni, consultare *Sezione 1, «HTTPD - Server web Apache2» [188]*.

Installare, su *server01*, munin. In un terminale, inserire:

```
sudo apt-get install munin
```

Su *server02*, installare il pacchetto munin-node:

```
sudo apt-get install munin-node
```

3.2. Configurazione

Su *server01* modificare il file `/etc/munin/munin.conf` aggiungendo l'indirizzo IP di *server02*:

```
## First our "normal" host.
[server02]
       address 172.18.100.101
```

Sostituire *server02* e *172.18.100.101* con il nome host e con l'indirizzo IP del proprio server.

Successivamente, configurare munin-node su *server02*. Modificare il file `/etc/munin/munin-node.conf` per consentire l'accesso al *server01*:

```
allow ^172\.18\.100\.100$
```

Sostituire *^172\.18\.100\.100$* con l'indirizzo IP del proprio server munin.

Riavviare munin-node su *server02* per applicare le modifiche:

```
sudo service munin-node restart
```

Infine, in un browser, inserire l'indirizzo *http://server01/munin* per visualizzare grafici che rappresentano le informazioni dal pacchetto *munin-plugins* standard per disco, rete, processi e sistema.

Poiché è una nuova installazione, potrebbe impiegare un po' di tempo affinché i grafici visualizzino qualche cosa di utile.

3.3. Plugin aggiuntivi

Il pacchetto munin-plugins-extra contiene controlli per le prestazioni e per servizi come DNS, DHCP, Samba e altri. Per installare il pacchetto, in un terminale inserire:

```
sudo apt-get install munin-plugins-extra
```

Assicurarsi di installare il pacchetto sia sul server che su tutti i nodi.

3.4. Riferimenti

- Per maggiori informazioni, consultare il sito web di *Munin*[5].
- In particolare, la pagina relativa *alla documentazione*[6] contiene informazioni su maggiori plugin, sulla scrittura di plugin, ecc..
- È anche disponibile un libro in tedesco da Open Source Press: *Munin Graphisches Netzwerk- und System-Monitoring*[7].
- Un'altra risorsa è la pagina della *documentazione della comunità su Munin*[8].

---

5 http://munin.projects.linpro.no/
6 http://munin.projects.linpro.no/wiki/Documentation
7 https://www.opensourcepress.de/index.php?26&backPID=178&tt_products=152
8 https://help.ubuntu.com/community/Munin

Capitolo 11. Server web

Un server web è un programma interattivo che accetta richieste HTTP da client, noti come browser web, e invia loro risposte HTTP insieme ad altri dati opzionali, di solito pagine web come documenti HTML e oggetti collegati (immagini, ecc.).

1. HTTPD - Server web Apache2

Apache è il server web più usato nei sistemi Linux; i server web sono usati per fornire pagine web richieste dai client. Normalmente i client richiedono e visualizzano pagine web usando applicazioni browser web come Firefox, Opera, Chromium o Mozilla.

Gli utenti digitano un Uniform Resource Locator (URL) per puntare a un server web attraverso il suo Fully Qualified Domain Name (FQDN) e il percorso della risorsa richiesta. Per esempio, per visualizzare la pagina iniziale del *sito web di Ubuntu*[1], un utente digiterà solo il FQDN:

```
www.ubuntu.com
```

Per visualizzare la pagina secondaria *comunità*[2], un utente digiterà il FQDN seguito da un percorso:

```
www.ubuntu.com/community
```

Il protocollo più utilizzato per il trasferimento delle pagine web è l'HTTP (Hyper Text Transfer Protocol). Sono anche supportati protocolli come HTTPS (Hyper Text Transfer Protocol over Secure Sockets Layer) e FTP (File Transfer Protocol), un protocollo per caricare e scaricare file dalla rete.

I server web Apache vengono comunemente usati in combinazione con il motore di database MySQL, il linguaggio di script per la pre-elaborazione dell'ipertesto PHP (Pre-processor Hyper Text) e altri noti linguaggi di script come Python e Perl. Questa configurazione viene denominata LAMP (Linux, Apache, MYSQL e Perl/Phyton/PHP) e costituisce una piattaforma robusta e potente per lo sviluppo e l'installazione di applicazioni basate sul web.

1.1. Installazione

Il server web Apache2 è disponibile in Ubuntu 10.04. Per installare Apache2:

- Al prompt di un terminale, eseguire il seguente comando:

  ```
  sudo apt-get install apache2
  ```

1.2. Configurazione

La configurazione di Apache2 avviene scrivendo delle *direttive* in semplici file di testo. Queste *direttive* sono suddivise tra i seguenti file e directory:

- *apache2.conf*: il principale file di configurazione di Apache2. Contiene impostazioni *globali* per Apache2.

[1] http://www.ubuntu.com
[2] http://www.ubuntu.com/community

- *conf.d*: contiene file di configurazione che si applicano *globalmente* ad Apache2. Altri pacchetti che usano Apache2 per fornire contenuti possono aggiungere file o collegamenti simbolici in questa directory.
- *envvars*: file dove vengono impostate le variabili *d'ambiente* di Apache2.
- *httpd.conf:* storicamente il principale file di configurazione di Apache2, prende il nome dal demone httpd. Adesso il file è generalmente vuoto, dato che la maggior parte delle opzioni di configurazione sono state spostate nelle directory riportate di seguito. Il file può essere usato per le opzioni di configurazione *specifiche dell'utente* che hanno effetto globalmente su Apache2.
- *mods-available*: questa directory contiene file di configurazione per caricare e configurare *moduli*. Non tutti i moduli hanno file di configurazione specifici.
- *mods-enabled*: contiene *collegamenti simbolici* ai file in `/etc/apache2/mods-available`. Quando viene creato un collegamento simbolico a un modulo di configurazione, viene abilitato al successivo riavvio di apache2.
- *ports.conf*: contiene le direttive che determinano su quali porte TCP Apache2 sta in ascolto.
- *sites-available*: questa directory contiene i file di configurazione per i *Virtual Hosts* di Apache2. Questi consentono di configurare Apache2 affinché venga utilizzato per siti multipli con configurazioni separate.
- *sites-enabled*: come mods-enabled, `sites-enabled` contiene collegamenti simbolici alla directory `/etc/apache2/sites-available`. Quando viene creato un collegamento simbolico di un file di configurazione nella directory sites-available, il sito configurato sarà attivo al riavvio di Apache2.

Altri file di configurazione possono essere aggiunti attraverso la direttiva *Include* e caratteri speciali possono essere usati per aggiungere molti altri file di configurazione. Una qualsiasi direttiva può essere posizionata in uno qualsiasi di questi file di configurazione. Modifiche ai file principali di configurazione vengono riconosciute solo con un riavvio di Apache2.

Il server legge anche un file contenente i tipi di documento mime; il nome del file è assegnato dalla direttiva *TypesConfig*, generalmente via `/etc/apache2/mods-available/mime.conf`, che può anche includere aggiunte e sostituzioni e per impostazione predefinita è `/etc/mime.types`.

1.2.1. Impostazioni di base

Questa sezione descrive i parametri di configurazione fondamentali del server Apache2. Per maggiori informazioni, consultare la *documentazione di Apache2*[3].

- Apache2 è dotato di una configurazione predefinita adatta agli host virtuali: è configurato con un singolo host virtuale (attraverso l'uso della direttiva *VirtualHost*) che può essere modificato oppure usato così com'è nel caso si disponga di un solo sito web oppure usato come modello per aggiungere altri host virtuali. Se lasciato così, l'host virtuale predefinito verrà usato come sito predefinito o come il sito che gli utenti vedranno se l'URL inserito non corrisponde alla direttiva

[3] http://httpd.apache.org/docs/2.2/

ServerName in uno qualsiasi dei file personalizzati. Per modificare l'host virtuale, modificare il file `/etc/apache2/sites-available/default`.

Le direttive impostate per un host virtuale si applicano solamente a quel particolare host. Se una direttiva è impostata all'interno del server e non è definita nelle impostazioni dell'host virtuale, vengono utilizzate le impostazioni predefinite. Per esempio, è possibile impostare un indirizzo email per il webmaster e non definirne alcuno per per gli host virtuali.

Per configurare un nuovo host virtuale o un nuovo sito, copiare quel file nella stessa directory con un nome a scelta. Per esempio:

```
sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mionuovosito
```

Modificare il file per configurare il nuovo sito usando alcune delle direttive descritte di seguito.

- La direttiva *ServerAdmin* specifica a quale indirizzo email il sistema deve indirizzare la posta destinata agli amministratori. Il valore predefinito è «webmaster@localhost». Quest'impostazione deve essere modificata con l'indirizzo che è stato assegnato all'utente (nel caso sia l'amministratore). Se il sito presenta dei problemi, Apache2 mostrerà un messaggio di errore indicante l'indirizzo a cui deve essere segnalato il problema. Questa direttiva è presente nel file /etc/apache2/sites-available del proprio sito.
- La direttiva *Listen* specifica la porta, e opzionalmente l'indirizzo IP, su cui Apache2 dovrebbe essere in ascolto. Se l'indirizzo IP non è specificato, Apache2 ascolta tutti gli indirizzi IP assegnati alla macchina. Il valore predefinito per la direttiva Listen è 80. Modificare questo valore, in 127.0.0.1:80 per fare in modo che Apache2 ascolti solo l'interfaccia di loopback e non sia disponibile verso internet, in 81 per modificare la porta di ascolto o lasciare il valore predefinito per il normale funzionamento. Questa direttiva può essere trovata e modifica in un file specifico: `/etc/apache2/ports.conf`
- La direttiva *ServerName* è opzionale e specifica il FQDN a cui il proprio sito risponde. L'host virtuale predefinito non ha la direttiva ServerName impostata, cosicché risponderà a tutte le richieste che non corrispondono alla direttiva ServerName in un altro host virtuale. Se si è i proprietari del dominio «ubunturocks.com» e si vuole ospitare tale dominio su un server Ubuntu, il valore della direttiva ServerName nel file di configurazione dell'host virtuale dovrebbe essere «ubunturocks.com». Aggiungere quindi questa direttiva al nuovo file di configurazione creato precedentemente (`/etc/apache2/sites-available/mionuovosito`).

  Potrebbe essere necessario che il proprio sito risponda anche alle richieste per «www.ubunturocks.com», dato che molti utenti ritengono corretto inserire il prefisso «www». Per ottenere questo, usare la direttiva *ServerAlias*: è possibile usare anche caratteri speciali con la direttiva ServerAlias.

  Per esempio, la seguente configurazione farà in modo che il proprio sito risponda a qualsiasi richiesta il cui dominio termina con *.ubunturocks.com*.

```
ServerAlias *.ubunturocks.com
```

- La direttiva *DocumentRoot* specifica dove Apache2 troverà i file che compongono il sito. Il valore predefinito è /var/www, come specificato in `/etc/apache2/sites-available/default`: è possibile modificare questo valore nel file di configurazione, ricordando di creare la directory, se necessario.

Abilitare il nuovo *VirtualHost* utilizzando l'utilità a2ensite e riavviare Apache2:

```
sudo a2ensite mionuovosito
sudo service apache2 restart
```

Assicurarsi di sostituire *mionuovosito* con una nome più descrittivo per il VirtualHost. Un metodo molto utilizzato consiste nel definire il nome del file secondo la direttiva *ServerName* dell'host virtuale.

Allo stesso modo, usare l'utilità a2dissite per disabilitare i siti. Questo può rivelarsi utile per diagnosticare problemi di configurazione con molteplici host virtuali:

```
sudo a2dissite mionuovosito
sudo service apache2 restart
```

1.2.2. Impostazioni predefinite

Questa sezione si occupa delle impostazioni predefinite del server Apache2. Per esempio, se viene aggiunto un host virtuale, le impostazioni modificate dell'host virtuale hanno precedenza rispetto quelle dell'host. Per una direttiva non definita, viene utilizzato il valore predefinito.

- *DirectoryIndex* è la pagina predefinita proposta dal server alle richieste dell'indice di una directory, specificate attraverso l'uso di una barra (/) come suffisso al nome della directory.

  Per esempio, quando un utente richiede la pagina http://www.example.com/questa_directory/, potrà ottenere la pagina DirectoryIndex, se questa esiste, un elenco di directory generato dal server, se la pagina non esiste ma l'opzione indexes è specificata, oppure una pagina di accesso negato se nessuna delle precedenti condizioni è vera. Il server cerca uno dei file elencati nella direttiva DirectoryIndex e restituisce il primo trovato. Se non trova nessuno di questi file e se *Options Indexes* è impostato per quella cartella, il server genera e restituisce un elenco, in formato HTML, delle sotto-directory e dei file contenuti nella directory. Il valore predefinito, presente in `/etc/apache2/mods-available/dir.conf`, è «index.html index.cgi index.pl index.php index.xhtml index.htm». Pertanto, se Apache2 trova nella directory indicata un file con uno di questi nomi, verrà visualizzato il primo.

- La direttiva *ErrorDocument* permette di specificare un file che sarà utilizzato da Apache2 per errori specifici. Per esempio, se un utente richiede una risorsa che non esiste, si verifica un errore 404: per impostazione predefinita Apache2 semplicemente restituisce un codice HTTP 404. Per maggiori informazioni sull'utilizzo di Error Document, comprese le posizioni dei file di esempio, consultare `/etc/apache2/conf.d/localized-error-pages`.

- Per impostazione predefinita il server scrive il log di trasferimento nel file `/var/log/apache2/access.log`: è possibile cambiare questo valore per ciascun sito nel file di configurazione dell'host virtuale con la direttiva *CustomLog*, oppure ometterlo per accettare il valore predefinito, specificato in `/etc/apache2/conf.d/other-vhosts-access-log`. È possibile anche specificare il file nel quale sono registrati gli errori tramite la direttiva *ErrorLog*, il cui valore predefinito è `/var/log/apache2/error.log`. Questi sono tenuti separati dai log di trasferimento per aiutare nella risoluzione di problemi con il server Apache2. È possibile inoltre specificare le direttive *LogLevel* (il valore predefinito è «warn») e *LogFormat* (visualizzare `/etc/apache2/apache2.conf` per conoscere il valore predefinito).
- Alcune opzioni vengono specificate per directory piuttosto che per server, come la direttiva *Options*. Una stanza «Directory» è racchiusa tra tag in stile XML:

```
<Directory /var/www/mionuovosito>
...
</Directory>
```

  La direttiva *Options* all'interno della stanza «Directory» accetta uno o più dei seguenti valori (tra gli altri) separati da spazi:

  - **ExecCGI**: consente l'esecuzione di script CGI. Questi script non vengono eseguiti se l'opzione non è selezionata.

    La maggior parte dei file non dovrebbe venir eseguita come script CGI, potrebbe essere molto pericoloso. Gli script CGI dovrebbero essere mantenuti in una directory separata, al di fuori della propria DocumentRoot e solo questa directory dovrebbe avere l'opzione ExecCGI impostata. Questo è il comportamento predefinito in Ubuntu e la posizione per gli script CGI è `/usr/lib/cgi-bin`.

  - **Includes**: consente inclusioni lato server, consente cioè a un file HTML di *contenere* altri file. Per maggiori informazioni, consultare la *Documentazione Apache SSI (comunità di Ubuntu)*[4].
  - **IncludesNOEXEC**: consente inclusioni lato server, ma disabilita i comandi *#exec* e *#include* negli script CGI.
  - **Indexes**: visualizza un elenco formattato dei contenuti della directory se non esiste alcun *DirectoryIndex* (come index.html) nella directory richiesta.

    Per motivi di sicurezza, quest'opzione non dovrebbe essere impostata e soprattutto non su DocumentRoot. Abilitare questa opzione con molta cautela solo su alcune directory e nel caso in cui si voglia visualizzare l'intero contenuto della directory.

  - **Multiview**: supporta visualizzazioni multiple in base al contenuto, quest'opzione è disabilitata in modo predefinito per ragioni di sicurezza. Per maggiori informazioni, consultare *la documentazione di Apache2*[5].
  - **SymLinksIfOwnerMatch**: segue i collegamenti simbolici solamente se il file di arrivo o la directory hanno gli stessi proprietari del collegamento.

---

[4] https://help.ubuntu.com/community/ServerSideIncludes

[5] http://httpd.apache.org/docs/2.2/mod/mod_negotiation.html#multiviews

1.2.3. Impostazioni di httpd

Questa sezione espone alcune delle configurazioni di base del demone httpd.

LockFile: la direttiva LockFile imposta il percorso al file di lock utilizzato quando il server viene compilato con USE_FCNTL_SERIALIZED_ACCEPT o USE_FLOCK_SERIALIZED_ACCEPT. Deve essere conservato nel disco locale. Questo valore dovrebbe essere lasciato invariato a meno che la directory di log non sia localizzata su una condivisione NFS. In questo caso, il valore dovrebbe essere modificato con una posizione sul disco locale e una directory accessibile solamente dall'utente root.

PidFile: la direttiva PidFile imposta il file in cui il server registra il proprio «pid». Questo file dovrebbe essere leggibile solamente dall'utente root. Nella maggior parte dei casi può essere lasciata invariata.

User: la direttiva User assegna l'identificativo dell'utente utilizzato dal server per rispondere alle richieste. Questa impostazione determina l'accesso al server: tutti i file inaccessibili per questo utente sono inaccessibili anche per i visitatori del sito; il valore predefinito per User è «www-data».

A meno che non sia estremamente necessario, non impostare mai la direttiva «User» a root. Utilizzare root con «User» può creare una falla nella sicurezza del server Web.

Group: la direttiva Group è simile alla direttiva User: stabilisce il gruppo le cui richieste ottengono risposta dal server; anche il gruppo predefinito è «www-data».

1.2.4. Moduli di Apache2

Apache2 è un server modulare: solo le funzionalità basilari sono incluse nel server principale. È possibile estendere le funzionalità del server attraverso dei moduli che vengono caricati all'interno di Apache2. Un piccolo insieme di moduli è incluso nel server durante la compilazione: se il server è compilato per caricare i moduli dinamicamente, gli stessi moduli possono essere compilati separatamente e aggiungi quando necessario utilizzando la direttiva LoadModule; altrimenti è necessario ricompilare Apache2 per aggiungere o rimuovere i moduli.

La versione di Ubuntu consente il caricamento dinamico dei moduli. Le direttive di configurazione possono essere incluse in base alla presenza di un particolare modulo racchiudendole in un blocco tipo: <*IfModulo*> block.

È quindi possibile installare moduli aggiuntivi di Apache2 e usarli con il server web. Per esempio, per installare il modulo *MySQL Authentication*, in un terminale digitare quanto segue:

```
sudo apt-get install libapache2-mod-auth-mysql
```

Per altri moduli, consultare la directory `/etc/apache2/mods-available`.

Usare l'utilità a2enmod per abilitare un modulo:

```
sudo a2enmod auth_mysql
sudo service apache2 restart
```

Allo stesso modo, a2dismod disabiliterà un modulo:

```
sudo a2dismod auth_mysql
sudo service apache2 restart
```

1.3. Configurazione HTTPS

Il modulo mod_ssl aggiunge un'importante caratteristica al server Apache2, l'abilità di cifrare le comunicazioni. In questo modo, quando il browser utilizza la cifratura SSL per le comunicazioni, il prefisso «https://» verrà inserito nell'URL (Uniform Resource Locator) nella barra degli indirizzi.

Il modulo mod_ssl è disponibile nel pacchetto apache2-common. Per abilitare il modulo mod_ssl, eseguire il seguente comando in un terminale:

```
sudo a2enmod ssl
```

Esiste un file di configurazione HTTPS predefinito in `/etc/apache2/sites-available/default-ssl`. Affinché Apache2 possa fornire connessioni HTTPS, sono necessari un *certificato* e una *chiave*. La configurazione HTTPS predefinita utilizza un certificato e una chiave generati attraverso ssl-cert, utili in fase di test, ma da sostituire con con una versione specifica per il sito o il server. Per maggiori informazioni su come generare una chiave e su come procurarsi un certificato, consultare *Sezione 5, «Certificati» [172]*

Per configurare l'HTTPS per Apache2, digitare quanto segue:

```
sudo a2ensite default-ssl
```

Le directory `/etc/ssl/certs` e `/etc/ssl/private` sono le posizioni predefinite. Se si installa il certificato e la chiave in un'altra directory assicurarsi di modificare *SSLCertificateFile* e *SSLCertificateKeyFile* appropriatamente.

Con l'HTTPS configurato, riavviare il servizio per abilitare le nuove impostazioni:

```
sudo service apache2 restart
```

In base a come è stato ottenuto il certificato, potrebbe essere necessario inserire una passphrase quando viene avviato Apache2.

È possibile accedere alle pagine del server sicuro digitando «https://nome_host/url/» nel barra degli indirizzi del proprio browser.

1.4. Condivisione del permesso di scrittura

Per consentire a più utenti di modificare la stessa directory è necessario concedere il permesso di scrittura a un gruppo al quale tutti appartengono. L'esempio seguente concede il permesso di scrittura di `/var/www` al gruppo «webmasters».

```
sudo chgrp -R webmasters /var/www
sudo find /var/www -type d -exec chmod g=rwxs "{}" \;
sudo find /var/www -type f -exec chmod g=rws "{}" \;
```

Se l'accesso deve essere concesso a più di un gruppo per directory, abilitare le Access Control List (ACL).

1.5. Riferimenti

- La *documentazione di Apache2*[6] contiene informazioni dettagliate riguardo le direttive di configurazione di Apache2. Inoltre, per la documentazione ufficiale di Apache2, consultare il pacchetto apache2-doc.
- Per maggiori informazioni riguardo SSL, consultare la *documentazione di Mod SSL*[7].
- Il libro *Apache Cookbook*[8] di O'Reilly è un'ottima risorsa per informazioni su specifiche configurazioni di Apache2.
- Per domande relative alla versione di Ubuntu di Apache2, chiedere nel canale IRC *#ubuntu-server* sul server *freenode.net*[9].
- Una buona risorsa riguardo PHP e MySQL può essere trovata nella *documentazione online*[10].

6 http://httpd.apache.org/docs/2.2/
7 http://www.modssl.org/docs/
8 http://oreilly.com/catalog/9780596001919/
9 http://freenode.net/
10 https://help.ubuntu.com/community/ApacheMySQLPHP

2. PHP5 - Linguaggio di scripting

PHP è un linguaggio di script universale pensato per lo sviluppo web. Uno script PHP può essere inserito direttamente nel codice HTML. Questa sezione spiega come installare e configurare PHP5 in sistemi Ubuntu con Apache2 e MySQL.

Questa sessione da per scontato che Apache2 e il server MySQL siano installati e configurati. Per maggiori informazioni sull'installazione e sulla configurazione dei due server, consultare la rispettiva documentazione presenti in questo documento.

2.1. Installazione

PHP5 è disponibile in Ubuntu: a differenza di python e perl, che sono installati nel sistema di base, PHP deve essere aggiunto.

- Per installare PHP5 è possibile digitare, in un terminale, quanto segue:

  ```
  sudo apt-get install php5 libapache2-mod-php5
  ```

  È possibile eseguire script di PHP5 dalla riga di comando installando il pacchetto php5-cli. Per installare php5-cli è sufficiente eseguire il seguente comando al prompt del terminale:

  ```
  sudo apt-get install php5-cli
  ```

  È possibile inoltre eseguire gli script di PHP5 senza installare il modulo PHP5 di Apache. Per fare ciò, è sufficiente installare il pacchetto php5-cgi digitando il seguente comando al prompt del terminale:

  ```
  sudo apt-get install php5-cgi
  ```

  Per usare MySQL con PHP5 è necessario installare il pacchetto php5-mysql. Per installare php5-mysql, eseguire il seguente comando al prompt del terminale:

  ```
  sudo apt-get install php5-mysql
  ```

  Allo stesso modo, per usare PostgreSQL con PHP5 è necessario installare il pacchetto php5-pgsql. Per installare php5-pgsql, eseguire il seguente comando al prompt del terminale:

  ```
  sudo apt-get install php5-pgsql
  ```

2.2. Configurazione

Una volta installato PHP5, è possibile eseguire gli script di PHP5 dal browser web. Se il pacchetto php5-cli è installato, è possibile eseguire gli script PHP5 dal prompt dei comandi.

Il server web Apache2 è configurato, in modo predefinito, per eseguire gli script di PHP5. In altre parole, il modulo PHP5 quando viene installato, viene abilitato automaticamente nel server web Apache2. Verificare che i file `/etc/apache2/mods-enabled/php5.conf` e `/etc/apache2/mods-enabled/php5.load` esistano. Se non dovessero esistere, è possibile abilitare il modulo usando il comando **a2enmod**.

Una volta installati i pacchetti correlati a PHP5 e abilitato il modulo PHP5 di Apache 2, è necessario riavviare Apache2 per eseguire script PHP5. È possibile eseguire il seguente comando nel terminale per riavviare il server web:

```
sudo service apache2 restart
```

2.3. Test

Per verificare l'installazione, è possibile eseguire la funzione «phpinfo» di PHP5 come segue:

```
<?php
  phpinfo();
?>
```

È sufficiente copiare il contenuto precedente in un file, come `phpinfo.php`, e salvarlo nella directory **DocumentRoot** del server web Apache2. Una volta puntato il browser web all'indirizzo `http://hostname/phpinfo.php`, dovrebbero venir visualizzati i valori di molti parametri di configurazione di PHP5.

2.4. Riferimenti

- Per ulteriori informazioni, consultare la documentazione di *php.net*[11].
- Esistono diversi libri su PHP. O'Reilly dispone di due ottimi libri: *Learning PHP 5*[12] e *PHP Cook Book*[13].
- Consultare anche la *documentazione online*[14].

[11] http://www.php.net/docs.php
[12] http://oreilly.com/catalog/9780596005603/
[13] http://oreilly.com/catalog/9781565926813/
[14] https://help.ubuntu.com/community/ApacheMySQLPHP

3. Squid - Server proxy

Squid è un potente proxy cache server che fornisce servizi proxy e cache per HTTP (Hyper Text Transport Protocol), FTP (File Transfer Protocol) e molti altri protocolli di rete. Squid può implementare servizi di caching e proxy anche per richieste SSL (Secure Sockets Layer), caching per ricerche di DNS (Domain Name Server) e fornire un caching trasparente. Squid supporta molti protocolli per il caching come ICP (Internet Cache Protocol), HTCP (Hyper Text Caching Protocol), CARP (Cache Array Routing Protocol) e WCCP (Web Cache Coordination Protocol).

Il server Squid è una valida soluzione per le necessità di caching e proxy, scala dall'utilizzo in un piccolo ufficio fino alla grande impresa, fornendo, attraverso il protocollo SNMP (Simple Network Management Protocol), un meccanismo di controllo e monitoraggio dei parametri critici molto accurato. Nella selezione di un computer da utilizzare come procy Squid dedicato, o come server cache, assicurarsi che il sistema sia equipaggiato con una grande quantità di memoria fisica, dal momento che Squid mantiene un cache in memoria per aumentare le prestazioni.

3.1. Installazione

Per installare il server Squid, da terminale digitare:

```
sudo apt-get install squid
```

3.2. Configurazione

La configurazione di Squid avviene attraverso la modifica di alcune direttive presenti nel file `/etc/squid/squid.conf`. Gli esempi che seguono descrivono alcune delle direttive che possono essere modificate. Per maggiori informazioni sulla configurazione di Squid consultare la sezione «Riferimenti».

Prima di modificare il file di configurazione, è utile farne una copia e proteggerla dalla scrittura così, in caso di necessità, è possibile utilizzare il file originale.

Copiare il file `/etc/squid/squid.conf` e proteggerlo dalla scrittura utilizzando i seguenti comandi:

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original
sudo chmod a-w /etc/squid/squid.conf.original
```

- Per impostare il server Squid affinché stia in ascolto sulla porta 8888 invece che sulla porta predefinita 3128, modificare la direttiva http_port:

  ```
  http_port 8888
  ```

- Modificare la direttiva visible_hostname per dare a Squid uno specifico hostname. Questo nome non deve essere necessariamente il nome del computer. Nell'esempio seguente è impostato a *weezie*

```
visible_hostname weezie
```

- Utilizzando il controllo di accessi Squid, è possibile configurare l'utilizzo dei servizi internet in proxy con Squid perché siano disponibili solo agli utenti con determinati Internet Protocol (IP). Per esempio, per consentire l'accesso solo agli utenti della sottorete 192.168.42.0/24:

  Aggiungere quanto segue alla **fine** della sezione ACL del file `/etc/squid/squid.conf`:

  ```
  acl fortytwo_network src 192.168.42.0/24
  ```

  Quindi aggiungere quanto segue all'**inizio** della sezione http_access del file `/etc/squid/squid.conf`:

  ```
  http_access allow fortytwo_network
  ```

- Using the excellent access control features of Squid, you may configure use of Internet services proxied by Squid to be available only during normal business hours. For example, we'll illustrate access by employees of a business which is operating between 9:00AM and 5:00PM, Monday through Friday, and which uses the 10.1.42.0/24 subnetwork:

  Aggiungere quanto segue alla **fine** della sezione ACL del file `/etc/squid/squid.conf`:

  ```
  acl biz_network src 10.1.42.0/24
  acl biz_hours time M T W T F 9:00-17:00
  ```

  Quindi aggiungere quanto segue all'**inizio** della sezione http_access del file `/etc/squid/squid.conf`:

  ```
  http_access allow biz_network biz_hours
  ```

Una volta apportate le modifiche al file `/etc/squid/squid.conf`, salvarlo e, per rendere effettivi i cambiamenti, riavviare squid utilizzando il comando:

```
sudo service squid restart
```

3.3. Riferimenti

Sito web di Squid[15]

Pagina della *documentazione online di Squid*[16].

[15] http://www.squid-cache.org/

[16] https://help.ubuntu.com/community/Squid

4. Ruby on Rails

Ruby on Rails è un ambiente web open source, per sviluppare applicazioni web che si avvalgono di database. È ottimizzato per la produttività sostenibile del programmatore dato che richiede di scrivere codice favorendo le convenzioni piuttosto che le configurazioni.

4.1. Installazione

Prima di installare Rails è necessario installare Apache e MySQL. Per installare il pacchetto Apache fare riferimento alla *Sezione 1, «HTTPD - Server web Apache2» [188]*, per MySQL fare riferimento alla *Sezione 1, «MySQL» [207]*.

Una volta installati Apache e MySQL, è possibile installare il pacchetto Ruby on Rails.

Per installare i pacchetti base di Ruby, digitare in un terminale il seguente comando:

```
sudo apt-get install rails
```

4.2. Configurazione

Modificare il file di configurazione `/etc/apache2/sites-available/default` per impostare i propri domini.

La prima cosa da cambiare è la direttiva *DocumentRoot*:

```
DocumentRoot /percorso/applicazione/rails/publicc
```

Successivamente, modificare <Directory "/percorso/applicazione/rails/public">:

```
<Directory "/percorso/applicazione/rails/public">
        Options Indexes FollowSymLinks MultiViews ExecCGI
        AllowOverride All
        Order allow,deny
        allow from all
        AddHandler cgi-script .cgi
</Directory>
```

È utile anche abilitare il modulo mod_rewrite di Apache. Per abilitare il modulo mod_rewrite, digitare il seguente comando in un terminale:

```
sudo a2enmod rewrite
```

Infine, è necessario modificare i proprietari delle directory `/percorso/applicazione/rails/public` e `/percorso/applicazione/rails/tmp` con il proprietario usato per eseguire il processo Apache:

```
sudo chown -R www-data:www-data /percorso/applicazione/rails/public
sudo chown -R www-data:www-data /percorso/applicazione/rails/tmp
```

Il server è ora pronto per le applicazioni Ruby on Rails.

4.3. Riferimenti

- Per ulteriori informazioni, consultare il *sito web di Ruby on Rails*[17].
- Anche *Agile Development with Rails*[18] è un'ottima risorsa.
- Un altro posto per reperire maggiori informazioni è la pagina della *documentazione della comunità di Ruby on Rails*[19].

[17] http://rubyonrails.org/
[18] http://pragprog.com/titles/rails3/agile-web-development-with-rails-third-edition
[19] https://help.ubuntu.com/community/RubyOnRails

5. Apache Tomcat

Apache Tomcat è un «contenitore» web che consente di servire Java Servlets e applicazioni web JSP (Java Server Pages).

I pacchetti Tomcat 6.0 in Ubuntu supportano due diverse modalità di esecuzione. È possibile installarli come una classica unica istanza globale, che viene lanciata all'avvio del sistema ed eseguita come utente senza privilegi tomcat6, ma è anche possibile installare istanze private che vengono eseguite con i diritti del proprio utente e che possono essere avviate e fermate dall'utente stesso. Questa seconda modalità è particolarmente utile nel contesto di un server di sviluppo nel quale più utenti hanno bisogno di testare le proprie istanze private Tomcat.

5.1. Installazione globale

Per installare il server Tomcat, digitare il seguente comando nel terminale:

```
sudo apt-get install tomcat6
```

In questo modo verrà installato il server Tomcat con un'applicazione web predefinita che visualizza una semplice pagina «It works».

5.2. Configurazione

I file di configurazione di Tomcat possono essere trovati in `/etc/tomcat6`. In questa sezione verranno spiegate solo alcune modifiche, per maggiori informazioni, consultare la *documentazione di Tomcat 6.0*[20].

5.2.1. Modificare la porta predefinita

Tomcat 6.0 esegue un connettore HTTP sulla porta 8080 e un connettore AJP sulla porta 8009; potrebbe essere utile modificare queste porte per evitare conflitti con altri server all'interno del sistema. Per fare questo, basta modificare le seguenti righe nel file `/etc/tomcat6/server.xml`:

```
<Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
...
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

5.2.2. Cambiare la JVM usata

Tomcat viene eseguito preferibilmente con OpenJDK-6, quindi con la JVM di Sun e infine con altre JVM. Se sono installate diverse JVM, è possibile impostare quale usare modificando la variabile JAVA_HOME nel file `/etc/default/tomcat6`:

[20] http://tomcat.apache.org/tomcat-6.0-doc/index.html

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

5.2.3. Dichiarare utenti e ruoli

Nomi utente, password e ruoli (gruppi) possono essere definiti in un contenitore Servlet. Con Tomcat 6.0 questo è fatto nel file `/etc/tomcat6/tomcat-users.xml`:

```
<role rolename="admin"/>
<user username="tomcat" password="s3cret" roles="admin"/>
```

5.3. Usare le applicazioni web standard di Tomcat

Tomcat dispone di applicazioni web che è possibile installare per documentarsi, per l'amministrazione o solo per dimostrazione.

5.3.1. Documentazione di Tomcat

Il pacchetto tomcat6-docs contiene la documentazione di Tomcat 6.0 sotto forma di applicazione web a cui è possibile accedere all'indirizzo «http://IL_PROPRIO_SERVER:8080/docs». È possibile installare il pacchetto attraverso il seguente comando:

```
sudo apt-get install tomcat6-docs
```

5.3.2. Applicazioni web amministrative di Tomcat

Il pacchetto tomcat6-admin contiene due applicazioni web che possono essere usate per amministrare il server Tomcat attraverso un'interfaccia web. È possibile installarle attraverso il seguente comando:

```
sudo apt-get install tomcat6-admin
```

La prima applicazione è il cosiddetto *manager*, a cui è possibile accedere dall'indirizzo «http://IL_PROPRIO_SERVER:8080/manager/html». È principalmente usata per ottenere informazioni sul server e riavviare le applicazioni web.

L'accesso al *manager* è protetto: è necessario definire un utente con il ruolo di «manager» nel file `/etc/tomcat6/tomcat-users.xml` prima di potervi accedere:

La seconda applicazione è l'*host-manager* a cui è possibile accedere attraverso l'indirizzo «http://IL_PROPRIO_SERVER:8080/host-manager/html». È possibile usarla per creare host virtuali dinamicamente.

Anche l'accesso all'applicazione *host-manager* è protetto: è necessario definire un utente con il ruolo di «admin» nel file `/etc/tomcat6/tomcat-users.xml` prima di potervi accedere.

Per motivi di sicurezza, l'utente tomcat6 non può scrivere nella directory `/etc/tomcat6` e alcune di queste applicazioni di amministrazione (produzione delle applicazioni, creazione di host virtuali)

necessitano di accesso in scrittura in tale directory. Per poter usare queste caratteristiche, eseguire i seguenti comandi per dare agli utenti del gruppo tomcat6 i permessi necessari:

```
sudo chgrp -R tomcat6 /etc/tomcat6
sudo chmod -R g+w /etc/tomcat6
```

5.3.3. Applicazioni web di esempio

Il pacchetto tomcat6-examples contiene due applicazioni web che possono essere usate per verificare o dimostrare le Servlet o le caratteristiche di JSP e sono accessibile dall'indirizzo «http://IL_PROPRIO_SERVER:8080/examples». Per installarle, usare il seguente comando:

```
sudo apt-get install tomcat6-examples
```

5.4. Usare istanze private

Tomcat è spesso usato in ambienti di sviluppo e di test dove usare una singola istanza all'interno del sistema non risulta molto utile ai molteplici utenti che sfruttano il sistema. I pacchetti di Tomcat 6.0 sono dotati di strumenti che facilitano la creazione di istanze dedicate a ogni singolo utente, consentendo, all'interno del sistema, di eseguire (senza i privilegi di root) istanze private e separate usando però sempre le librerie di sistema.

È possibile eseguire le istanze globali e private in parallelo, basta solo che non usino le stesse porte TCP.

5.4.1. Installare il supporto alle istanze private

È possibile installare tutto il necessario per eseguire istanze private attraverso il seguente comando:

```
sudo apt-get install tomcat6-user
```

5.4.2. Creare un'istanza privata

È possibile creare un'istanza privata attraverso il seguente comando:

```
tomcat6-instance-create mia-istanza
```

In questo modo verrà creata una nuova directory `mia-istanza` con tutte le sottodirectory e gli script necessari. Sarà poi possibile installare le librerie comuni nella sottodirectory `lib/` e sviluppare le proprie applicazioni in `webapps/`. Non vi è alcuna applicazione predefinita in questa directory.

5.4.3. Configurare un'istanza privata

I file di configurazione di Tomcat per un'istanza privata sono disponibili nella sottodirectory `conf/`. È necessario modificare, per esempio, il file `conf/server.xml` per modificare le porte predefinite

usate dall'istanza privata di Tomcat per evitare conflitti con altre istanze che potrebbero essere in esecuzione.

5.4.4. Avviare e fermare un'istanza privata

È possibile avviare un'istanza privata utilizzando il seguente comando (si presuppone che l'istanza sia posizionata nella directory `mia-istanza`):

```
mia-istanza/bin/startup.sh
```

Controllare la sottodirectory `logs/` per la presenza di errori. Se si nota un errore del tipo «*java.net.BindException: Address already in use<null>:8080*», significa che la porta in uso è già utilizzata ed è necessario modificarla.

Per fermare un'istanza, usare il seguente comando (si presuppone che l'istanza sia posizionata nella directory `mia-istanza`):

```
mia-istanza/bin/shutdown.sh
```

5.5. Riferimenti

- Per ulteriori informazioni, consultare il *sito web di Apache Tomcat*[21].
- Il libro *Tomcat: The Definitive Guide*[22] è un'ottima risorsa per creare siti web con Tomcat.
- Per ulteriori libri, consultare la pagina *Tomcat Books*[23].
- Consultare anche la *documentazione online della comunità di Apache Tomcat*[24].

[21] http://tomcat.apache.org/
[22] http://oreilly.com/catalog/9780596003180/
[23] http://wiki.apache.org/tomcat/Tomcat/Books
[24] https://help.ubuntu.com/community/ApacheTomcat5

Capitolo 12. Database

Ubuntu fornisce due dei più popolari server database:

- MySQL™
- PostgreSQL

Questi sono disponibili nel repository «main». La seguente sezione descrive come installare e configurare questi database.

1. MySQL

MySQL è un veloce e robusto database SQL multi-thread e multi-utente. È concepito per funzionare in situazioni critiche, sistemi di produzione a elevato carico e anche per essere inserito in software destinato alla distribuzione di massa.

1.1. Installazione

Per installare MySQL, eseguire il seguente comando dal terminale:

```
sudo apt-get install mysql-server
```

In Ubuntu 12.04, MySQL è installato per impostazione predefinita. Anche se è comptatibile al 100% con MySQL 5.1, se dovesse sorgere la necessità di installare quest'ultima versione (per esempio per servire da secondario per altri server MySQL 5.1), si può installare appunto il pacchetto mysql-server-5.1.

Durante l'installazione viene chiesto di inserire una password per l'utente root di MySQL.

Una volta completata l'installazione, il server MySQL dovrebbe avviarsi automaticamente. È possibile digitare i seguenti comandi in un terminale per controllare se il server è in esecuzione:

```
sudo netstat -tap | grep mysql
```

L'output del comando precedente dovrebbe essere:

```
tcp 0 0 localhost:mysql *:* LISTEN 2556/mysqld
```

Se il server non funziona correttamente, è possibile digitare il seguente comando per avviarlo:

```
sudo service mysql restart
```

1.2. Configurazione

Per configurare le impostazioni di base (file di registrazione, numero porta, ecc...), è possibile modificare il file `/etc/mysql/my.cnf`. Per esempio, per configurare MySQL affinché ascolti le connessioni dagli host nella rete, modificare la direttiva *bind-address* con l'indirizzo IP del server:

```
bind-address            = 192.168.0.5
```

Sostituire 192.168.0.5 con l'indirizzo appropriato.

Dopo aver modificato `/etc/mysql/my.cnf`, è necessario riavviare il demone MySQL:

```
sudo service mysql restart
```

Per modificare la password *root* di MySQL, in un terminale digitare:

```
sudo dpkg-reconfigure mysql-server-5.5
```

Il demone MySQL viene arrestato, e viene chiesto di inserire una nuova password.

1.3. Macchine per database

Nonostante la configurazione predefinita di MySQL fornita dai pacchetti Ubuntu sia perfettamente funzionante e fornisca buone prestazioni, sono necessarie alcune considerazioni prima di proseguire.

MySQL è progettato per memorizzare i dati in modi diversi: questi metodi sono riferiti sia al database che alle macchine di salvataggio dei dati; ci sono principalmente due macchine che possono risultare interessanti: InnoDB e MyISAM. Le macchine di memorizzazione sono trasparenti per l'utente finale: MySQL funzionerà diversamente sotto la superficie ma, indipendentemente da quale macchina stia usando, l'interazione con il database sarà la stessa.

Ogni macchina ha vantaggi e svantaggi.

È possibile, e potrebbe portare a dei vantaggi, combinare e confrontare le macchine per database a livello di tabella, ma questo riduce l'effettività dell'ottimizzazione delle prestazioni, in quanto si divideranno le risorse tra due macchine, invece di dedicarsi a solo una di esse.

- MyISAM è il più vecchio dei due, in certe circostanze può essere più veloce di InnoDB e preferisce un carico di lavoro in sola lettura. Alcune applicazioni web sono state calibrate su MyISAM (sebbene ciò non implica che sarebbero più lente con InnoDB). MyISAM supporta anche il tipo di dati FULLTEXT, che consente di effetture veloci ricerche in grandi quantità di dati testuali. Tuttavia MyISAM può effettuare il lock di scrittura solo a livello dell'intera tabella: ciò significa che solo un processo per volta può aggiornare una tabella e quando le applicazioni che usano la tabella aumentano, ciò può costituire un ostacolo. Manca anche della funzione di journaling, il che rende più difficile il recupero dei dati dopo un crash. Il seguente link fornisce alcune considerazioni sull'uso di *MyISAM su un database in ambiente di produzione*[1].
- InnoDB è una macchina per database più moderna, progettata per essere *conforme «ACID»*[2] e ciò garantisce che le transazioni del database siano processate in modo affidabile. Il lock di scrittura può essere gestito a livello di riga entro una tabella e questo significa che possono essere effettuati contemporaneamente aggiornamenti multipli su una singola tabella. La cache dei dati è anche gestita in memoria all'interno della macchina, consentendo la stessa a un più efficiente livello di riga piuttosto che per blocco di file. Per conformarsi alle proprietà «ACID», il journaling di tutte le transazioni per le principali tabelle è effettuato in maniera indipendente. Questo consente un recupero dei dati più affidabile, in quanto può essere controllata la consistenza dei dati.

---

[1] http://www.mysqlperformanceblog.com/2006/06/17/using-myisam-in-production/

[2] http://en.wikipedia.org/wiki/ACID

MySQL 5.5 è la macchina predefinita e si suggerisce di usare questa anzichè MyISAM, a meno che non ci sia uno specifico bisogno delle caratteristiche proprie di quest'ultima macchina.

1.4. Configurazione avanzata

1.4.1. Creare un file my.cnf calibrato

È possibile regolare diversi parametri nel file di configurazione di MySQL, per migliorare le prestazioni del server. Per un'impostazione iniziale, può essere utile lo *strumento di generazione del file my.cnf di Percona*[3]. Questo strumento sarà di ausilio nella creazione di un file my.cnf ottimizzato per le caratteristiche specifiche del server in uso e le necessità dell'utente.

Non sostituire il file my.cnf esistente con quello di Percona se sono stati già caricati dati nel database. Alcuni dei cambiamenti apportati al file saranno incompatibili, in quanto alterano la maniera in cui i dati vengono memorizzati sul disco fisso e quindi non sarà possibile avviare MySQL. Se è necessario usarlo, e nel database sono già presenti dei dati, è necessario effettuare un mysqldump e ricaricare:

```
mysqldump --all-databases --all-routines -u root -p > ~/fulldump.sql
```

Viene richiesta la password di amministratore prima di creare una copia dei dati. Assicurarsi che nessun altro utente o processo stiano usando il database durante questa operazione. A seconda della quantità di dati presenti nel database, l'operazione potrebbe richiedere un certo periodo di tempo; durante il procedimento sullo schermo non si vedrà nulla.

Una volta completato lo scarico, chiudere MySQL:

```
sudo service mysql stop
```

Effettuare un backup del file my.cnf originale e sostituirlo con quello nuovo:

```
sudo cp /etc/my.cnf /etc/my.cnf.backup
sudo cp /path/to/new/my.cnf /etc/my.cnf
```

Quindi cancellare e reinizializzare il database, assicurandosi che i diritti di proprietà siano corretti prima di riavviare MySQL:

```
sudo rm -rf /var/lib/mysql/*
sudo mysql_install_db
sudo chown -R mysql: /var/lib/mysql
sudo service start mysql
```

Rimane solo da reimportare i dati; per avere un'idea dello stato di avanzamento del processo può essere usata l'utilità «pv», la pipe di visualizzazione. Quanto segue illustra come installare e usare «pv» in questo caso, ma se si preferisce non usarlo, è possibile sostituire «pv» con «cat» nel seguente

[3] http://tools.percona.com/members/wizard

comando. Ignorare gli orari ETA prodotti da «pv», perché sono basati sulla media dei tempi necessari per gestire ogni riga del file, ma la velocità d'inserimento può variare i maniera considerevole da riga a riga con mysqldump:

```
sudo apt-get install pv
pv ~/fulldump.sql | mysql
```

Una volta completato, è tutto pronto a partire!

Questo non è necessario per tutte le modifiche di my.cnf; molte delle variabili da modificare per migliorare le prestazioni sono regolabili anche durante il funzionamento del server. Come sempre, assicurarsi di avere una buona copia di backup dei file di configurazione e dei dati, prima di apportare modifiche.

1.4.2. MySQL Tuner

MySQL Tuner è un utile strumento che si connette a un'istanza MySQL in esecuzione e offre suggerimenti su come ottimizzarne la configurazione per l'attuale carico di lavoro. Quanto più esteso è il periodo di funzionamento del server, tanto migliori risulteranno i suggerimenti di mysqltuner: in un ambiente di produzione, far trascorrere almeno 24 ore prima di avviare lo strumento. È possibile scaricare e installare mysqltuner dai repository Ubuntu:

```
sudo apt-get install mysqltuner
```

Dopo averlo installato, lanciarlo:

```
mysqltuner
```

e aspettare il rapporto finale. La sezione superiore fornisce infomrazioni generali sul server di database, e la parte conclusiva i suggerimenti sulle regolazioni del file my.cnf, molte delle quali possono essere effettuate durante il funzionamento del server, senza necessità di riavvio; consultare la documentazione ufficiale di MySQL (link nella sezione Risorse) per informazioni sulle variabili rilevanti da modificare in produzione. Quanto segue è parte di un rapporto di esempio in un database di produzione che evidenzia benefici derivanti da un aumento della cache per le query:

```
-------- Recommendations -----------------------------------------------------
General recommendations:
Run OPTIMIZE TABLE to defragment tables for better performance
Increase table_cache gradually to avoid file descriptor limits
Variables to adjust:
key_buffer_size (> 1.4G)
query_cache_size (> 32M)
table_cache (> 64)
innodb_buffer_pool_size (>= 22G)
```

Un commento finale sulla regolazione dei database: nonostante si possa generalmente affermare che determinate impostazioni siano le migliori, le prestazioni possono variare da un'applicazione all'altra.

Per esempio, ciò che funziona meglio per Wordpress potrebbe non esserlo per Drupla, Joomla o software proprietario. Le prestazioni dipendono dai tipi di query, dall'uso di indici, dall'efficienza della progettazione del database e così via; può essere utile cercare suggerimenti sulla regolazione del database basati sulle applicazioni in uso. Raggiunto un determinato livello, qualunque regolazione effettuata può solo condurre a miglioramenti minimi e sarebbe meglio migliorare l'applicazione o cercare di potenziare l'ambiente del database, sia usando hardware più potente che aggiungendo server secondari.

1.5. Risorse

- Per maggiori informazioni, consultare *il sito web di MySQL*[4].
- Documentazione completa è disponibile sia online che in formati offline nel portale degli *Sviluppatori di MySQL*[5].
- Per informazioni generali su SQL, consultare *Using SQL Special Edition*[6] di Rafe Colburn.
- Ulteriori informazioni sono disponibili nella *documentazione online*[7].

[4] http://www.mysql.com/
[5] http://dev.mysql.com/doc/
[6] http://www.informit.com/store/product.aspx?isbn=0768664128
[7] https://help.ubuntu.com/community/ApacheMySQLPHP

2. PostgreSQL

PostgreSQL è un database relazionale orientato agli oggetti che presenta le caratteristiche di un database commerciale tradizionale e anche miglioramenti dei sistemi DBMS di prossima generazione.

2.1. Installazione

Per installare PostgreSQL, eseguire il seguente comando dal terminale:

```
sudo apt-get install postgresql
```

Una volta che l'installazione è completata, è possibile configurare il server PostgreSQL a seconda delle proprie esigenze, sebbene la configurazione predefinita sia abbastanza buona.

2.2. Configurazione

By default, connection via TCP/IP is disabled. PostgreSQL supports multiple client authentication methods. IDENT authentication method is used for postgres and local users, unless otherwise configured. Please refer *the PostgreSQL Administrator's Guide if you would like to configure alternatives like Kerberos*[8].

The following discussion assumes that you wish to enable TCP/IP connections and use the MD5 method for client authentication. PostgreSQL configuration files are stored in the `/etc/postgresql/<version>/main` directory. For example, if you install PostgreSQL 9.1, the configuration files are stored in the `/etc/postgresql/9.1/main` directory.

To configure *ident* authentication, add entries to the `/etc/postgresql/9.1/main/pg_ident.conf` file. There are detailed comments in the file to guide you.

To enable TCP/IP connections, edit the file `/etc/postgresql/9.1/main/postgresql.conf`

Localizzare la riga *#listen_addresses = 'localhost'* e modificarla in:

```
listen_addresses = 'localhost'
```

Per consentire ad altri computer di collegarsi al server PostgreSQL, sostituire «localhost» con l'*indirizzo IP* del server, o in alternativa «0.0.0.0» per associarlo a tutte le interfacce.

Tutti gli altri parametri possono essere modificati, ma bisogna sapere cosa si sta facendo. Per maggiori informazioni, consultare la documentazione di PostgresSQL o fare riferimento ai file di configurazione.

Ora che è possibile collegarsi al server PostgreSQL, è necessario impostare una password per l'utente *postgres*. In un terminale, eseguire il seguente comando per connettersi al modello di database predefinito di PostgreSQL:

[8] http://www.postgresql.org/docs/9.1/static/admin.html

```
sudo -u postgres psql template1
```

Il comando precedente connette al database PostreSQL *template1* come l'utente *postgres*. Una volta collegati al server PostgreSQL, si sarà al prompt SQL. È possibile eseguire il seguente comando SQL al prompt psql per configurare la password per l'utente *postgres*.

```
ALTER USER postgres with encrypted password 'TUA_PASSWORD';
```

After configuring the password, edit the file `/etc/postgresql/9.1/main/pg_hba.conf` to use *MD5* authentication with the *postgres* user:

```
local   all         postgres                          md5
```

Infine, riavviare il servizio PostgreSQL per inizializzare la nuova configurazione. In un terminale, digitare quanto segue per riavviare PostgreSQL:

```
sudo service postgresql-8.4 restart
```

The above configuration is not complete by any means. Please refer *the PostgreSQL Administrator's Guide*[9] to configure more parameters.

2.3. Risorse

- As mentioned above the *Administrator's Guide*[10] is an excellent resource. The guide is also available in the postgresql-doc-9.1 package. Execute the following in a terminal to install the package:

  ```
  sudo apt-get install postgresql-doc-9.1
  ```

  To view the guide enter **file:///usr/share/doc/postgresql-doc-9.1/html/index.html** into the address bar of your browser.

- Per informazioni generali riguardo SQL, consultare *Using SQL Special Edition*[11] di Rafe Colburn.
- Per maggiori informazioni, consultare anche la *documentazione online riguardo PostgreSQL*[12].

[9] http://www.postgresql.org/docs/9.1/static/admin.html
[10] http://www.postgresql.org/docs/9.1/static/admin.html
[11] http://www.informit.com/store/product.aspx?isbn=0768664128
[12] https://help.ubuntu.com/community/PostgreSQL

Capitolo 13. Applicazioni LAMP

1. Panoramica

Le installazioni LAMP (Linux + Apache + MySQL + PHP/Perl/Python) sono molto diffuse sui server Ubuntu ed esistono moltissime applicazioni open source scritte utilizzando questa infrastruttura. Alcune di queste applicazioni sono: wiki, CMS (Content Management Systems) e software di gestione come phpMyAdmin.

Uno dei vantaggi dell'infrastruttura LAMP è la sua flessibilità nell'utilizzo di diversi tipi di database, server web e linguaggio di script. Al posto di MySQL è possibile quindi usare Postgresql o SQLite, Python, Perl e Ruby vengono spesso utilizzati al posto di PHP mentre Nginx, Cherokee e Lighttpd possono sostituire Apache.

Il modo più rapido per iniziare è installare LAMP usando tasksel, uno strumento Debian/Ubuntu che installa nel sistema diversi pacchetti tra loro collegati come «task» coordinati. Per installare un server LAMP:

- Al prompt di un terminale, eseguire il seguente comando:

```
sudo tasksel install lamp-server
```

Terminata questa installazione, è possibile installare molte applicazioni *LAMP* nel seguente modo:

- Scaricare un archivio contenente il codice sorgente dell'applicazione.
- Estrarre l'archivio in una directory accessibile a un server web.
- In base a dove è stato estratto il codice sorgente, configurare un server web per fornire questi file.
- Configurare l'applicazione affinché si colleghi al database.
- Eseguire uno script o spostarsi su una pagina dell'applicazione per installare il database necessario all'applicazione.
- Completati i passi precedenti, o dei passi simili, è possibile utilizzare l'applicazione.

Esistono anche alcuni svantaggi con questo approccio: i file delle applicazioni non sono organizzati all'interno del file system in modo standard causando confusione sul dove è stata installata l'applicazione. Inoltre, l'aggiornamento dell'applicazione risulta essere complicato: quando viene rilasciata una nuova versione, è necessario ripetere gli stessi passi per l'installazione.

Molte applicazioni *LAMP* sono comunque disponibili all'interno dei repository di Ubuntu e si installano come tutte le altre normali applicazioni. In base però all'applicazione, potrebbe essere necessario apportare alcune configurazioni in più una volta installate.

Questa sezione illustra come installare alcune applicazioni *LAMP*.

2. Moin Moin

MoinMoin è un motore per wiki scritto in Python, basato sul motore «PikiPiki» e rilasciato sotto licenza GNU GPL.

2.1. Installazione

Per installare MoinMoin, eseguire il seguente comando al prompt:

```
sudo apt-get install python-moinmoin
```

È necessario installare anche il server web apache2. Per installare apache-2, consultare la sottosezione *Sezione 1.1, «Installazione» [188]* della sezione *Sezione 1, «HTTPD - Server web Apache2» [188]* .

2.2. Configurazione

Per configurare per la prima volta un wiki, chiamato per esempio *mywiki*, eseguire i seguenti comandi:

```
cd /usr/share/moin
sudo mkdir mywiki
sudo cp -R data mywiki
sudo cp -R underlay mywiki
sudo cp server/moin.cgi mywiki
sudo chown -R www-data.www-data mywiki
sudo chmod -R ug+rwX mywiki
sudo chmod -R o-rwx mywiki
```

È ora necessario configurare MoinMoin affinché identifichi il nuovo wiki *mywiki*. Per configurare MoinMoin, aprire il file `/etc/moin/mywiki.py` e modificare la riga:

```
data_dir = '/org/mywiki/data'
```

in

```
data_dir = '/usr/share/moin/mywiki/data'
```

Inoltre, al di sotto dell'opzione *data_dir*, aggiungere *data_underlay_dir*:

```
data_underlay_dir='/usr/share/moin/mywiki/underlay'
```

Se il file `/etc/moin/mywiki.py` non esiste, è necessario copiare il file `/usr/share/moin/config/wikifarm/mywiki.py` nel file `/etc/moin/mywiki.py` ed eseguire la modifica descritta precedentemente.

Se il nome del wiki è *my_wiki_name*, è necessario inserire nel file `/etc/moin/farmconfig.py` questa riga «("my_wiki_name", r".*")» subito dopo la riga «("mywiki", r".*")».

Una volta configurato MoinMoin per trovare il wiki chiamato *mywiki*, è necessario configurare apache2 in modo che gestisca anche i wiki.

Aggiungere le seguenti righe nel file `/etc/apache2/sites-available/default` all'interno della sezione «<VirtualHost *>»

```
### moin
  ScriptAlias /mywiki "/usr/share/moin/mywiki/moin.cgi"
  alias /moin_static193 "/usr/share/moin/htdocs"
  <Directory /usr/share/moin/htdocs>
  Order allow,deny
  allow from all
  </Directory>
### end moin
```

Una volta configurato apache2, è necessario riavviarlo. Per riavviare il server web apache2, digitare:

```
sudo service apache2 restart
```

2.3. Verifica

Per verificare se l'applicazione wiki funziona, è sufficiente aprire con un browser web il seguente URL:

```
http://localhost/mywiki
```

Per ulteriori dettagli, consultare il sito web di *MoinMoin*[1].

2.4. Riferimenti

- Per maggiori informazioni, consultare il *wiki di MoinMoin*[2].
- È possibile anche consultare la pagina della *documentazione della comunità su MoinMoin*[3].

[1] http://moinmo.in/
[2] http://moinmo.in/
[3] https://help.ubuntu.com/community/MoinMoin

3. MediaWiki

MediaWiki è un software per wiki scritto con il linguaggio PHP ed è in grado di utilizzare database come MySQL o PostgreSQL per l'archiviazione dei dati.

3.1. Installazione

Prima di installare MediaWiki è necessario installare Apache2, il linguaggio PHP5 e un sistema di database. MySQL o PostgreSQL sono i più comuni, sceglierne uno in base alle proprie necessità. Per le istruzioni su come installarli, fare riferimento alle relative sezioni all'interno di questa guida.

Per installare MediaWiki, eseguire il seguente comando al prompt:

```
sudo apt-get install mediawiki php5-gd
```

Per maggiori informazioni sulle funzionalità di MediaWiki, consultare il pacchetto mediawiki-extensions.

3.2. Configurazione

Il file di configurazione di Apache `mediawiki.conf` per MediaWiki è installato nella directory `/etc/apache2/conf.d/`. Da questo file, per poter accedere all'applicazione MediaWiki, è utile togliere il commento alla seguente riga.

```
# Alias /mediawiki /var/lib/mediawiki
```

Una volta tolto il commento alla riga precedente, riavviare il server Apache e accedere a MediaWiki utilizzando il seguente URL:

```
http://localhost/mediawiki/config/index.php
```

Consultare la sezione «Checking environment...» presente in quella pagina. È possibile risolvere molti problemi leggendola attentamente.

Una volta completata la configurazione, copiare il file `LocalSettings.php` nella directory `/etc/mediawiki`.

```
sudo mv /var/lib/mediawiki/config/LocalSettings.php /etc/mediawiki/
```

Può anche essere necessario modificare `/etc/mediawiki/LocalSettings.php` per impostare il limite di memoria (disabilitato per impostazione predefinita):

```
ini_set( 'memory_limit', '64M' );
```

3.3. Estensioni

Le estensioni aggiungono nuove funzionalità a MediaWiki e forniscono agli amministratori del wiki e agli utenti l'abilità di personalizzare MediaWiki in base alle loro necessità.

È possibile scaricare estensioni per MediaWiki come un archivio o direttamente dal repository Subversion copiandolo nella directory `/var/lib/mediawiki/extensions` directory. Alla fine del file aggiungere la seguente riga: `/etc/mediawiki/LocalSettings.php`.

```
require_once "$IP/extensions/ExtentionName/ExtentionName.php";
```

3.4. Riferimenti

- Per maggiori informazioni, consultare il *sito web di MediaWiki*[4].
- La *MediaWiki Administrators' Tutorial Guide*[5] contiene molte informazioni per i nuovi amministratori di MediaWiki.
- Anche la pagina della *documentazione della comunità su MediaWiki*[6] è una buona risorsa.

[4] http://www.mediawiki.org
[5] http://www.packtpub.com/Mediawiki/book
[6] https://help.ubuntu.com/community/MediaWiki

4. phpMyAdmin

phpMyAdmin è un'applicazione LAMP sviluppata appositamente per amministrare server MySQL. Scritta in PHP e accessibile attraverso un browser web, fornisce un'interfaccia grafica per svolgere attività di amministrazione su un database.

4.1. Installazione

Prima di poter installare phpMyAdmin, è necessario poter accedere al database MySQL o dallo stesso host in cui phpMyAdmin è installato o da un host accessibile via rete (per maggiori informazioni, consultare *Sezione 1, «MySQL» [207]*). Da un terminale, digitare:

```
sudo apt-get install phpmyadmin
```

Al prompt dei comandi, scegliere quale server web configurare per phpMyAdmin. Nel resto di sezione sezione viene utilizzato Apache2.

All'interno di un browser, nella barra degli indirizzi, scrivere *http://NOMESERVER/phpmyadmin*, sostituendo *NOMESERVER* con il vero nome dell'host. Alla schermata di accesso, scrivere *root* per *username* o un altro utente MySQL e digitare MySQL per la password.

Una volta effettuato l'accesso, è possibile modificare la password di *root*, creare utenti e creare ed eliminare database, tabelle, ecc...

4.2. Configurazione

I file di configurazione di phpMyAdmin sono posizionati in `/etc/phpmyadmin`. Il file principale di configurazione è `/etc/phpmyadmin/config.inc.php` e contiene le opzioni globali di phpMyAdmin.

Per utilizzare phpMyAdmin per l'amministrazione di un database MySQL presente in un altro server, modificare le seguenti opzioni nel file `/etc/phpmyadmin/config.inc.php`:

```
$cfg['Servers'][$i]['host'] = 'db_server';
```

Sostituire *db_server* con il vero nome del server in cui è presente il database remoto oppure con il suo indirizzo IP. Inoltre, assicurarsi che l'host in cui è presente phpMyAdmin possa accedere al database remoto.

Una volta configurato, terminare e ricominciare la sessione di phpMyAdmin per poter accedere al nuovo server.

I file `config.header.inc.php` e `config.footer.inc.php` vengono usati per aggiungere un'intestazione e un pedice HTML a phpMyAdmin.

Un altro importante file di configurazione è `/etc/phpmyadmin/apache.conf`, un collegamento simbolico al file `/etc/apache2/conf.d/phpmyadmin.conf`, usato per configurare Apache2 affinché

visualizzi phpMyAdmin. Nel file sono presenti le direttive per il caricamento di PHP, i permessi per la directory, ecc... Per maggiori informazioni sulla configurazione di Apache2, consultare *Sezione 1, «HTTPD - Server web Apache2» [188]*.

4.3. Riferimenti

- La documentazione di phpMyAdmin è installata automaticamente con il pacchetto ed è possibile accedervi dal collegamento *phpMyAdmin Documentation* (un punto di domanda) al di sotto del logo di phpMyAdmin. La documentazione ufficiale può anche essere visualizzata direttamente dal *sito di phpMyAdmin*[7].
- Inoltre, il libro *Mastering phpMyAdmin*[8] è un'ottima fonte per reperire ulteriori informazioni.
- Una terza risorsa è la pagina della *documentazione della comunità su phpMyAdmin*[9].

[7] http://www.phpmyadmin.net/home_page/docs.php
[8] http://www.packtpub.com/phpmyadmin-3rd-edition/book
[9] https://help.ubuntu.com/community/phpMyAdmin

Capitolo 14. Server di file

Se si dispone di più di un computer su una singola rete, a un certo punto potrebbe essere necessario condividere dei file tra questi computer. In questa sezione viene spiegato come installare e configurare servizi come FTP, NFS e CUPS.

1. Server FTP

File Transfer Protocol (FTP) è un protocollo TCP per scaricare file tra computer: in passato è stato usato anche per il caricamento ma, considerato che questo metodo non utilizza la cifratura, sia le credenziali dell'utente che i dati sono trasferiti in chiaro e facilmente intercettati. Se si cerca un modo per caricare e scaricare file in maniera sicura, consultare la sezione OpenSSH in *Capitolo 6, Amministrazione remota [81]*.

FTP opera con un modello client/server: la componente server è chiamata *demone FTP*, che resta in ascolto di richieste FTP da parte di client remoti. Alla ricezione di una richiesta, gestisce l'autenticazione e attiva la connessione; per la durata della connessione esegue i comandi inviati dai client FTP.

L'accesso a un server FTP può essere gestito in due modi:

- Anonimo
- Con autenticazione

Nella modalità anonima, i client remoti possono accedere al server FTP usando l'account predefinito «anonymous» o «ftp» e usando come password un indirizzo email; nella modalità autenticata, un utente deve avere un account e una password: quest'ultima scelta è molto poco sicura e non dovrebbe essere usata se non in speciali circostanze. Se è necessario trasferire file in sicurezza, cercare SFTP nella sezione sui server Open-SSH. L'accesso alle directory e ai file nel server FTP dipende dai permessi definiti per l'account usato per l'accesso. Come regola generale, il demone FTP nasconde la directory root del server FTP e la modifica con la directory home di FTP, nascondendo così il resto del file system dalle sessioni remote.

1.1. vsftpd - Installazione del server FTP

Un demone FTP disponibile in Ubuntu è vsftpd: è semplice da installare, configurare e mantenere. È possibile installare vsftpd eseguendo il seguente comando:

```
sudo apt-get install vsftpd
```

1.2. Configurazione anonima di FTP

Per impostazione predefinita, vsftpd *non* è configurato per consentire di scaricare file in maniera anonima: per abilitare lo scaricamento anonimo modificare `/etc/vsftpd.conf` cambiando:

```
anonymous_enable=Yes
```

Durante l'installazione viene creato un utente *ftp* con una directory home di `/srv/ftp`; questa è la directory FTP predefinita.

Se è necessario modificare questa posizione, per esempio in `/srv/files/ftp`, creare semplicemente una directory in un'altra posizione e modificare la directory home dell'utente *ftp*:

```
sudo mkdir /srv/files/ftp
sudo usermod -d /srv/files/ftp ftp
```

Applicate le modifiche, riavviare vsftpd:

```
sudo restart vsftpd
```

Infine, copiare i file e le directory da rendere disponibili attraverso FTP anonimo in `/srv/files/ftp` o `/srv/ftp`, per utilizzare l'impostazione predefinita.

1.3. Configurazione FTP per utenti autenticati

Per impostazione predefinita vsftpd è configurato per autenticare gli utenti di sistema e consentire loro di scaricare file: per consentire agli utenti di caricare file, modificare `/etc/vsftpd.conf`:

```
write_enable=YES
```

Riavviare vsftpd:

```
sudo restart vsftpd
```

Ora, quando gli utenti accedono via FTP, il loro punto di partenza sarà la propria directory *home*, dove potranno scaricare e caricare file e creare directory.

Allo stesso modo, per impostazione predefinita, gli utenti anonimi non possono caricare file nel server FTP: per modificare questa impostazione, occorre togliere il commento alla riga seguente e riavviare vsftpd:

```
anon_upload_enable=YES
```

Abilitare il caricamento anonimo di file via FTP può compromettere la sicurezza del sistema. È sconsigliato abilitare il caricamento anonimo su server collegati direttamente a Internet.

Il file di configurazione è composto da diversi parametri di configurazione, le cui informazioni sono disponibili nel file stesso. In alternativa, è possibile fare riferimento alla pagina man (**man 5 vsftpd.conf**).

1.4. FTP sicuro

All'interno del file di configurazione `/etc/vsftpd.conf` di vsftpd, sono presenti molte opzioni per rendere il programma più sicuro. Per esempio, togliendo il commento a quanto segue, gli utenti possono essere limitati all'utilizzo solo della propria directory personale:

```
chroot_local_user=YES
```

È anche possibile limitare un particolare gruppo di utenti all'utilizzo delle sole directory personali:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

Tolto il commento alle opzioni precedenti, creare un file `/etc/vsftpd.chroot_list` con l'elenco degli utenti, uno per riga, quindi riavviare vsftpd:

```
sudo restart vsftpd
```

Inoltre, il file `/etc/ftpusers` contiene un elenco di utenti a cui è *negato* l'accesso FTP. L'elenco comprende gli utenti root, daemon, nobody, ecc... Per disabilitare l'accesso FTP ad altri utenti, aggiungerli semplicemente a questo elenco.

Il protocollo FTP può anche essere cifrato utilizzando *FTPS*: a differenza di *SFTP*, *FTPS* è FTP su Secure Socket Layer (SSL), mentre *SFTP* è una sessione FTP all'interno di una connessione cifrata con *SSH*. La principale differenza consiste nel fatto che gli utenti SFTP devono avere un account *shell* sul sistema, invece di una shell *nologin*. Fornire però una shell a tutti gli utenti potrebbe non essere sempre applicabile in alcuni ambienti, come nei casi di servizio di host web. È tuttavia possibile restringere tali account unicamente a SFTP e disabilitare l'interazione shell: per maggiori particolari, consultare la sezione sui server OpenSSH.

Per configurare *FTPS*, modificare il file `/etc/vsftpd.conf` aggiungendo:

```
ssl_enable=Yes
```

Inoltre, notare anche le opzioni relative al certificato e alla chiave:

```
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

In modo predefinito queste opzioni sono impostate nel certificato e nella chiave forniti dal pacchetto ssl-cert: in un ambiente di produzione queste dovrebbero essere sostituite con un certificato e una chiave generati per l'host specifico. Per ulteriori informazioni sui certificati, consultare *Sezione 5, «Certificati» [172]*.

Riavviare vsftpd e gli utenti non-anonimi utilizzeranno *FTPS*:

```
sudo restart vsftpd
```

Per consentire accesso FTP agli utenti dotati di una shell `/usr/sbin/nologin`, ma non dispongono di accesso shell, modificare il file `/etc/shells` aggiungendo *nologin*:

```
# /etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/screen
/usr/sbin/nologin
```

Questo è necessario poiché, in modo predefinito, vsftpd utilizza PAM per l'autenticazione e i file di configurazione `/etc/pam.d/vsftpd` contiene:

```
auth    required        pam_shells.so
```

Il modulo *shells* di PAM limita l'accesso alle shell indicate nel file `/etc/shells`.

Molti popolari client FTP possono essere configurati per utilizzare connessioni FTPS: il client a riga di comando lftp è in grado di utilizzare FTPS.

1.5. Riferimenti

- Per maggiori informazioni, consultare il *sito web di vsftpd*[1].
- For detailed `/etc/vsftpd.conf` options see the *vsftpd.conf man page*[2].

[1] http://vsftpd.beasts.org/vsftpd_conf.html
[2] http://manpages.ubuntu.com/manpages/quantal/en/man5/vsftpd.conf.5.html

2. NFS (Network File System)

NSF permette a un sistema di condividere file e directory con altri attraverso una rete. Utilizzando NFS, utenti e programmi possono accedere ai file presenti su sistemi remoti come se fossero dei file locali.

Alcuni dei principali benefici forniti da NFS sono:

- Le workstation locali utilizzano meno spazio su disco perché i dati comuni possono essere memorizzati su una singola macchina, pur rimanendo accessibili agli altri attraverso la rete.
- Gli utenti non devono avere diverse directory home su ciascuna macchina in rete. Le directory home possono risiedere sul server NFS ed essere rese disponibili attraverso la rete.
- I dispositivi di archiviazione come dischi floppy, unità CD-ROM e USB possono essere utilizzate dagli altri computer della rete. Questo può ridurre il numero di unità per supporti rimovibili presenti nella rete.

2.1. Installazione

Per installare il server NFS, inserire il comando seguente a un prompt di terminale:

```
sudo apt-get install nfs-kernel-server
```

2.2. Configurazione

È possibile configurare le directory da esportare aggiungendole al file `/etc/exports`. Per esempio:

```
/ubuntu *(ro,sync,no_root_squash)
/home *(rw,sync,no_root_squash)
```

È possibile sostituire * con uno qualsiasi dei formati per i nomi di host. È necessario rendere la dichiarazione dei nomi di host più specifica possibile per impedire l'accesso di sistemi indesiderati ai mount NFS.

Per avviare il server NFS, è possibile eseguire il seguente comando a un prompt di terminale:

```
sudo service nfs-kernel-server start
```

2.3. Configurazione client NFS

Utilizzare il comando mount per montare una directory NFS condivisa da un'altra macchina, digitando un comando simile al seguente a un prompt di terminale:

```
sudo mount esempio.nomehost.it:/ubuntu /locale/ubuntu
```

Il punto di mount `/locale/ubuntu` deve esistere. Non ci dovrebbero essere né file, né sottodirectory all'interno di `/locale/ubuntu`.

Un modo alternativo per montare una condivisione NFS da un'altra macchina consiste nell'aggiungere una riga al file `/etc/fstab`. Questa riga deve contenere il nome dell'host del server NFS, la directory esportata dal server e la directory sulla macchina locale dove montare la condivisione NFS.

La sintassi generale per la riga nel file `/etc/fstab` è come segue:

```
esempio.nomehost.it:/ubuntu /locale/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr
```

Se si hanno problemi nel montare la condivisione NFS, assicurarsi che il pacchetto nfs-common sia installato sul client. Per installare nfs-common, digitare il seguente comando al prompt del terminale:

```
sudo apt-get install nfs-common
```

2.4. Riferimenti

FAQ di NFS per Linux[3]

Documentazione online riguardo NFS[4]

[3] http://nfs.sourceforge.net/
[4] https://help.ubuntu.com/community/NFSv4Howto

3. Iniziatore iSCSI

iSCSI (Internet Small Computer System Interface) è un protocollo che permette di inviare comandi SCSI su di una rete. Tipicamente iSCSI è implementato in una SAN (Storage Area Network) per consentire al server di accedere a una grande riserva di spazio su disco fisso. Il protocollo iSCSI fa riferimento ai client come *iniziatori* e ai server iSCSI come *target*.

Ubuntu Server può essere configurato sia come iniziatore che come target iSCSI: questa guida fornisce i comandi e le opzioni di configurazione per impostare un iniziatore iSCSI. Si presume che sia già presente un target iSCSI sulla rete locale e che si abbiano i diritti appropriati per connettersi. Le istruzioni per impostare un target variano grandemente tra i fornitori di hardware e si consiglia di consultare la documentazione del fornitore per configurare uno specifico target iSCSI.

3.1. Installazione dell'iniziatore iSCSI

Per configurare Ubuntu Server come iniziatore iSCSI, installare il pacchetto open-iscsi, digitando in un terminale:

```
sudo apt-get install open-iscsi
```

3.2. Configurazione dell'iniziatore iSCSI

Una volta installato il pacchetto open-iscsi, modificare `/etc/iscsi/iscsid.conf` come segue:

```
node.startup = automatic
```

È possibile controllare quali target sono disponibili usando l'utilità iscsiadm, digitando in un terminale:

```
sudo iscsiadm -m discovery -t st -p 192.168.0.10
```

- *-m:* determina la modalità di esecuzione di iscsiadm.
- *-t:* specifica il tipo di discovery.
- l'opzione *-p:* definisce l'indirizzo IP del target.

Modificare il valore d'esempio *192.168.0.10* nell'indirizzo IP del target della rete.

Se il target è disponibile, dovrebbe essere visualizzato un output simile al seguente:

```
192.168.0.10:3260,1 iqn.1992-05.com.emc:sl7b92030000520000-2
```

Il valore di *iqn* e l'indirizzo IP sopra riportati possono variare in relazione alle componenti hardware utilizzate.

È possibile ora connettersi al target iSCSI e, in relazione alle sue impostazioni, può essere necessario digitare le proprie credenziali. Effettuare l'accesso al nodo iSCSI:

```
sudo iscsiadm -m node --login
```

Controllare che il nuovo disco sia stato riconosciuto utilizzando dmesg:

```
dmesg | grep sd
```

```
[ 4.322384] sd 2:0:0:0: Attached scsi generic sg1 type 0
[ 4.322797] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[ 4.322843] sd 2:0:0:0: [sda] Write Protect is off
[ 4.322846] sd 2:0:0:0: [sda] Mode Sense: 03 00 00 00
[ 4.322896] sd 2:0:0:0: [sda] Cache data unavailable
[ 4.322899] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 4.323230] sd 2:0:0:0: [sda] Cache data unavailable
[ 4.323233] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 4.325312] sda: sda1 sda2 < sda5 >
[ 4.325729] sd 2:0:0:0: [sda] Cache data unavailable
[ 4.325732] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 4.325735] sd 2:0:0:0: [sda] Attached SCSI disk
[ 2486.941805] sd 4:0:0:3: Attached scsi generic sg3 type 0
[ 2486.952093] sd 4:0:0:3: [sdb] 1126400000 512-byte logical blocks: (576 GB/537 GiB)
[ 2486.954195] sd 4:0:0:3: [sdb] Write Protect is off
[ 2486.954200] sd 4:0:0:3: [sdb] Mode Sense: 8f 00 00 08
[ 2486.954692] sd 4:0:0:3: [sdb] Write cache: disabled, read cache: enabled, doesn't
 support DPO or FUA
[ 2486.960577] sdb: sdb1
[ 2486.964862] sd 4:0:0:3: [sdb] Attached SCSI disk
```

Nell'output sopra riportato, *sdb* è il nuovo disco iSCSI; ricordare che questo è solo un esempio, l'output visualizzato può essere diverso.

Creare quindi una partizione, formattare il file system e montare il nuovo disco iSCSI. Digitare in un terminale:

```
sudo fdisk /dev/sdb
n
p
invio
w
```

I comandi sopra riportati sono relativi all'utilità fdisk; per più dettagliate istruzioni, consultare la pagina di manuale: **man fdisk**. L'utilità cfdisk offre un'interfaccia più semplice.

Formattare ora il file system e montarlo per esempio in `/srv`:

```
sudo mkfs.ext4 /dev/sdb1
```

```
sudo mount /dev/sdb1 /srv
```

Infine, aggiungere una voce in `/etc/fstab` per montare il disco iSCSI all'avvio:

```
/dev/sdb1 /srv ext4 defaults,auto,_netdev 0 0
```

È una buona idea assicurarsi che tutto funzioni come previsto riavviando il sistema.

3.3. Riferimenti

Sito Open-iSCSI[5]

Pagina Debian Open-iSCSI[6]

5 http://www.open-iscsi.org/
6 http://wiki.debian.org/SAN/iSCSI/open-iscsi

4. CUPS - Server di stampa

Il sistema primario e i servizi di stampa di Ubuntu sono gestiti da **Common UNIX Printing System** (CUPS). Questo è un sistema di stampa liberamente disponibile e altamente portabile ed è diventato il nuovo standard per la stampa in molte distribuzioni Linux.

CUPS gestisce lavori e code di stampa, fornisce la stampa in rete tramite l'utilizzo del protocollo IPP (Internet Printing Protocol) e al tempo stesso offre supporto a una nutrita schiera di stampanti, dalle quelle a matrice di punti a quelle al laser (comprese tutte quelle nel mezzo). CUPS supporta anche il PPD (PostScript Printer Detection) e il rilevamento automatico delle stampanti di rete; inoltre fornisce un semplice strumento di amministrazione e configurazione basato sul web.

4.1. Installazione

Per installare CUPS nel proprio computer Ubuntu, basta usare sudo con il comando apt-get e fornire i pacchetti da installare come primo parametro. Un'installazione completa di CUPS ha molte dipendenze di pacchetti, ma possono essere specificati tutti nella stessa riga di comando. Digitare quello che segue al prompt del terminale per installare CUPS:

```
sudo apt-get install cups
```

Dopo essersi autenticati con la propria password utente, i pacchetti dovrebbero essere scaricati e installati. Completato questo processo, il server CUPS viene avviato automaticamente.

Per la risoluzione dei problemi, è possibile accedere alle registrazioni degli errori attraverso il file `/var/log/cups/error_log`. Se non vengono mostrate informazioni sufficienti per risolvere i problemi incontrati, è possibile incrementare la prolissità delle registrazioni del server CUPS modificando la direttiva **LogLevel** nel file di configurazione dal valore predefinito «info» a «debug» oppure «debug2», che registra tutto. Se vengono apportate ulteriori modifiche, ricordarsi di ripristinare i valori iniziali una volta risolto il problema per evitare di ritrovarsi file di registrazione di notevoli dimensioni

4.2. Configurazione

Il comportamento del server CUPS viene configurato attraverso le direttive contenute nel file `/etc/cups/cupsd.conf`. Il file di configurazione di CUPS segue la stessa sintassi del file di configurazione primario del server HTTP Apache. In questo modo, l'utente che ha familiarità con la modifica del file di configurazione di Apache si sentirà a suo agio nella modifica del file di configurazione di CUPS. Di seguito vengono presentati alcuni esempi di impostazioni che potrebbe essere opportuno cambiare fin da subito.

Prima di modificare il file di configurazione, è opportuno creare un copia del file originale e proteggerla da scrittura, in modo da avere le impostazioni originali come riferimento e per riusarle in caso di necessità.

Copiare il file `/etc/cups/cupsd.conf` e proteggerlo dalla scrittura con i seguenti comandi, inseriti a un prompt di terminale.

```
sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.original
sudo chmod a-w /etc/cups/cupsd.conf.original
```

- **ServerAdmin**: per configurare l'indirizzo email dell'amministratore del server CUPS, modificare il file di configurazione `/etc/cups/cupsd.conf` con un editor di testo e aggiungere o modificare la riga *ServerAdmin*. Per esempio, se si è amministratori del server CUPS e il proprio indirizzo email è «mario@example.net», modificare la riga ServerAdmin in questo modo:

  ```
  ServerAdmin mario@example.net
  ```

- **Listen**: in modo predefinito, su Ubuntu, l'installazione del server CUPS resta in ascolto solamente sull'interfaccia di loopback all'indirizzo IP *127.0.0.1*. Per poter fare in modo che il server CUPS ascolti sull'indirizzo IP della rete, è necessario specificare un nome host, l'indirizzo IP oppure una coppia indirizzo IP/porta con l'aggiunta di una direttiva «Listen». Per esempio, se il server CUPS è all'interno di una rete locale all'indirizzo IP *192.168.10.250* e si desidera renderlo accessibile ad altri sistemi in questa sotto-rete, è necessario modificare il file `/etc/cups/cupsd.conf` e aggiungere una direttiva «Listen» in questo modo:

  ```
  Listen 127.0.0.1:631 # Listen esistente per loopback
  Listen /var/run/cups/cups.sock # socket Listen esistente
  Listen 192.168.10.250:631 # Listen sull'interfaccia LAN, porta 631 (IPP)
  ```

  Nell'esempio precedente, è possibile rendere un commento o rimuovere il riferimento all'indirizzo di loopback (127.0.0.1) se non si desidera che cupsd resti in ascolto su quell'interfaccia, ma che invece resti in ascolto solo sull'interfaccia Ethernet della LAN (Local Area Network). Per abilitare l'ascolto su tutte le interfacce di rete a cui un certo host è collegato, inclusa quella di loopback, è possibile creare una voce Listen per l'host *socrates* come segue:

  ```
  Listen socrates:631 # Listen su tutte le interfacce dell'host "socrates"
  ```

  oppure omettendo la direttiva Listen e utilizzando quella *Port*, come in:

  ```
  Port 631 # Listen sulla porta 631 di tutte le interfacce
  ```

Per ulteriori esempi di direttive di configurazione nel file di configurazione del server CUPS, consultare la pagina manuale associato inserendo il comando seguente a un prompt di terminale:

```
man cupsd.conf
```

Ogni volta che vengono apportati cambiamenti al file di configurazione `/etc/cups/cupsd.conf`, è necessario riavviare il server CUPS digitando il comando seguente a un prompt di terminale:

```
sudo service cups restart
```

4.3. Interfaccia web

CUPS può essere configurato e monitorato utilizzando un'interfaccia web disponibile all'indirizzo *http://localhost:631/admin*. L'interfaccia web può anche essere usata per svolgere tutte le attività di gestione della stampante.

Per svolgere le attività di amministrazione attraverso l'interfaccia web, è necessario avere l'account root abilitato sul server o aver eseguito l'autenticazione con un utente nel gruppo *lpadmin*. Per motivi di sicurezza, CUPS non autentica gli utenti provi di password.

Per aggiungere un utente al gruppo *lpadmin*, eseguire il seguente comando in un terminale:

```
sudo usermod -aG lpadmin username
```

Maggiore documentazione è disponibile nella scheda *Documentation/Help* dell'interfaccia web.

4.4. Riferimenti

Sito Web di CUPS[7]

Pagina Debian Open-iSCSI[8]

---

[7] http://www.cups.org/

[8] http://wiki.debian.org/SAN/iSCSI/open-iscsi

Capitolo 15. Servizi email

Il processo per portare una email da una persona a un'altra all'interno di una rete o attraverso internet, comporta l'utilizzo di diversi sistemi che cooperano tra loro. Ognuno di questi sistemi deve essere configurato correttamente. Colui che spedisce una email utilizza un *Mail User Agent* (MUA), o client email, per spedire il messaggio attraverso uno o più *Mail Transfer Agents* (MTA), l'ultimo dei quali lo consegnerà a un *Mail Delivery Agent* (MDA) per la consegna nella casella di posta del destinatario, che la preleverà utilizzando un client email attraverso un server POP3 o IMAP.

1. Postfix

Postfix è il Mail Transfer Agent (MTA) predefinito di Ubuntu. Cerca di essere facile da amministrare e sicuro ed è compatibile con l'MTA sendmail. Questa sezione espone come installare e configurare postfix e anche come configurare un server SMTP utilizzando un collegamento sicuro (per l'invio di email in sicurezza).

Questa guida non spiega come configurare *Virtual Domains* di Postfix. Per informazioni sui Virtual Domains e altre configurazioni avanzate, consultare *Sezione 1.7.3, «Riferimenti» [242]*.

1.1. Installazione

Per installare postfix eseguire il seguente comando:

```
sudo apt-get install postfix
```

Premere «Invio» quando il processo di installazione pone delle domande, la configurazione verrà effettuata in dettaglio al passo successivo.

1.2. Configurazione di base

Per configurare postfix, eseguire il seguente comando:

```
sudo dpkg-reconfigure postfix
```

Viene visualizzata l'interfaccia utente. In ogni schermata selezionare i seguenti valori:

- Internet Site
- mail.example.com
- steve
- mail.example.com, localhost.localdomain, localhost
- No
- 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/24
- 0
- +
- tutti

Sostituire mail.example.com con il dominio con cui si accettano email, 192.168.0.0/24 con l'intervallo di rete e di classe del proprio server mail e steve con il nome utente appropriato.

A questo punto è utile decidere quale formato usare per la mailbox. Postfix, come impostazione predefinita, utilizza **mbox** come formato. Invece di modificare il file di configurazione, è possibile usare il comando **postconf** per configurare tutti i parametri di postfix che vengono salvati nel file

`/etc/postfix/main.cf`. Per riconfigurare un particolare parametro, è sempre possibile eseguire il comando precedente o modificare il file.

Per configurare la casella di posta per **Maildir**:

```
sudo postconf -e 'home_mailbox = Maildir/'
```

Questo posizionerà le nuove mail in /home/*NOME_UTENTE*/Maildir e sarà quindi necessario configurare il proprio MDA (Mail Delivery Agent) affinché utilizzi lo stesso percorso.

1.3. Autenticazione SMTP

SMTP-AUTH consente a un client di identificarsi attraverso un meccanismo di autenticazione (SASL). TLS (Transport Layer Security) dovrebbe essere usato per cifrare il processo di autenticazione. Una volta autenticato, il server SMTP consentirà ai client di scaricare le email.

1. Configurare Postfix per SMTP-AUTH usando SASL (Dovecot SASL):

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth-client'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions = \
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
```

La configurazione *smtpd_sasl_path* è un percorso relativo alla directory di Postfix.

2. Ora, ottenere o generare un certificato digitale per TLS; per maggiori informazioni consultare la sezione *Sezione 5, «Certificati» [172]*. In questo esempio viene usata anche un'Autorità di Certificazione (CA); per informazioni su come generare un certificato CA, consultare la sezione *Sezione 5.5, «Autorità di Certificazione» [174]*.

Il MUA che si connette al server mail ha bisogno di riconoscere il certificato usato per TLS. Ciò può essere ottenuto sia usando un certificato proveniente da una CA commerciale che con un certificato auto-firmato installato/accettato manualmente dall'utente. I certificati non sono mai validati da MTA a MTA TLS senza un preliminare accordo fra le organizzazioni interessate; a meno che politiche locali non lo richiedano, non c'è alcuna ragione per non usare certificati auto-firmati. Per ulteriori dettagli, fare riferimento a *Sezione 5.3, «Creare un certificato auto-firmato» [174]*

3. Ottenuto un certificato, configurare Postfix affinché fornisca cifratura TLS per le mail in entrate e in uscita:

```
sudo postconf -e 'smtp_tls_security_level = may'
sudo postconf -e 'smtpd_tls_security_level = may'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/server.key'
sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/server.crt'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'myhostname = mail.example.com'
```

4. Se si sta usando la propria *Autorità di Certificazione* per firmare il certificato, digitare:

```
sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
```

Di nuovo, per maggiori informazioni sui certificati, consultare *Sezione 5, «Certificati» [172]*.

Una volta eseguiti tutti i comandi, Postfix è configurato per SMTP-AUTH ed è stato creato un certificato auto-firmato per la cifratura TLS.

Ora, il file `/etc/postfix/main.cf` dovrebbe essere simile a *questo*[1].

La configurazione iniziale di postfix è completa, eseguire il seguente comando per riavviarne il demone:

```
sudo service postfix restart
```

Postfix supporta SMTP-AUTH come descritto in *RFC2554*[2] ed è basato su *SASL*[3]. È comunque ancora necessario impostare l'autenticazione SASL prima di poter usare SMTP-AUTH.

1.4. Configurare SASL

Postfix supporta due implementazioni SASL: Cyrus SASL e Dovecot SASL. Per abilitare Dovecot SASL è necessario installare il pacchetto dovecot-common. In un terminale digitare:

```
sudo apt-get install dovecot-common
```

Modificare quindi il file `/etc/dovecot/dovecot.conf`. Nella sezione *auth default* de-commentare l'opzione *socket listen* e modificare come di seguito:

```
socket listen {
  #master {
    # Master socket provides access to userdb information. It's typically
    # used to give Dovecot's local delivery agent access to userdb so it
    # can find mailbox locations.
    #path = /var/run/dovecot/auth-master
    #mode = 0600
```

1 ../sample/postfix_configuration
2 http://www.ietf.org/rfc/rfc2554.txt
3 http://www.ietf.org/rfc/rfc2222.txt

```
      # Default user/group is the one who started dovecot-auth (root)
      #user =
      #group =
    #}
    client {
      # The client socket is generally safe to export to everyone. Typical use
      # is to export it to your SMTP server so it can do SMTP AUTH lookups
      # using it.
      path = /var/spool/postfix/private/auth-client
      mode = 0660
      user = postfix
      group = postfix
    }
  }
```

Affinché i client Outlook utilizzino SMTP-AUTH, nella sezione *auth default* di /etc/dovecot/dovecot.conf aggiungere *"login"*:

```
  mechanisms = plain login
```

Una volta configurato Dovecot, riavviarlo:

```
sudo service dovecot restart
```

1.5. Mail-Stack Delivery

Un'altra opzione per configurare Postfix per SMTP-AUTH è usare il pacchetto mail-stack-delivery (in precedenza disponibile come dovecot-postfix). Questo pacchetto installa Dovecot e configura Postfix per usarlo sia per autenticazione SASL che come Mail Delivery Agent (MDA). Il pacchetto configura anche Dovecot per IMAP, IMAPS, POP3 e POP3S.

L'esecuzione di IMAP, IMAPS, POP3, or POP3S sul server mail potrebbe eventualmente rendersi necessaria: per esempio, per configurare il server come gateway di posta, come filtro spam/virus, ecc.. In tal caso può essere più semplice usare i comandi sopra riportati per configurare Postfix per SMTP-AUTH.

Per installare il pacchetto, in un terminale digitare:

```
sudo apt-get install mail-stack-delivery
```

Il server mail dovrebbe essere funzionante, anche se è possibile modificarne ulteriormente la configurazione. Il pacchetto, per esempio, utilizza il certificato e la chiave presi dal pacchetto ssl-cert, ma con un server in produzione dovrebbero essere usati un certificato e una chiave generati appositamente per l'host. Per maggiori informazioni, consultare *Sezione 5, «Certificati» [172]*.

Ottenuto un certificato personalizzato e una chiave per l'host, modificare le seguenti opzioni nel file `/etc/postfix/main.cf`:

```
smtpd_tls_cert_file = /etc/ssl/certs/ssl-mail.pem
smtpd_tls_key_file = /etc/ssl/private/ssl-mail.key
```

Riavviare Postfix:

```
sudo service postfix restart
```

1.6. Test

La configurazione di SMTP-AUTH è completa ed è ora necessario provarla.

Per verificare se SMTP-AUTH e TLS funzionano correttamente, eseguire il seguente comando:

```
telnet mail.example.com 25
```

Una volta stabilita la connessione al server mail Postfix, digitare:

```
ehlo mail.example.com
```

Se, tra tutte le righe, viene visualizzato anche questo, allora funziona correttamente. Digitare **quit** per uscire.

```
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```

1.7. Risoluzione problemi

Questa sezione descrive alcuni metodi comuni per determinare la cause dei problemi che potrebbero verificarsi.

1.7.1. Evitare l'uso di chroot

Il pacchetto postfix di Ubuntu viene installato, in modo predefinito e per ragioni di sicurezza, all'interno di un ambiente *chroot*.

Per terminate l'operazione chroot, localizzare la seguente riga nel file `/etc/postfix/master.cf`:

```
smtp      inet  n       -       -       -       -       smtpd
```

e modicarlo come segue:

```
smtp      inet  n       -       n       -       -       smtpd
```

È necessario riavviare Postfix affinché utilizzi la nuova configurazione. In un terminale, digitare:

```
sudo service postfix restart
```

1.7.2. File di registro

Postfix invia tutti i messaggi di registrazione in `/var/log/mail.log`. I messaggi di errore e gli avvisi possono andar persi nell'output della registrazione normale, per questo vengono anche registrati in `/var/log/mail.err` e `/var/log/mail.warn` rispettivamente.

Per visualizzare in tempo reale i messaggi che vengono registrati, usare il comando tail -f:

```
tail -f /var/log/mail.err
```

Il livello di dettaglio delle registrazioni può essere incrementato. Di seguito vengono riportate alcune opzioni di configurazione per aumentare i dettagli di registrazione in alcune delle aree descritte precedentemente.

- Per aumentare la registrazione delle attività *TLS*, impostare l'opzione *smtpd_tls_loglevel* a un valore compreso tra 1 e 4.

  ```
  sudo postconf -e 'smtpd_tls_loglevel = 4'
  ```
- Se si riscontrano problemi nell'inviare o nel ricevere email da uno specifico dominio, è possibile aggiungere tale dominio al parametro *debug_peer_list*.

  ```
  sudo postconf -e 'debug_peer_list = problem.domain'
  ```
- È possibile incrementare il livello di registrazione di qualsiasi demone Postfix modificando il file `/etc/postfix/master.cf` e aggiungendo *-v* subito dopo la voce. Per esempio, modificare la voce *smtp*:

  ```
  smtp unix  - - - - - smtp -v
  ```

It is important to note that after making one of the logging changes above the Postfix process will need to be reloaded in order to recognize the new configuration: **sudo service postfix reload**

- Per incrementare il livello di informazioni registrate durante la risoluzione di problemi con *SASL*, è possibile impostare le seguenti opzioni nel file `/etc/dovecot/dovecot.conf`

  ```
  auth_debug=yes
  auth_debug_passwords=yes
  ```

Just like Postfix if you change a Dovecot configuration the process will need to be reloaded: **sudo service dovecot reload**.

Alcune delle opzioni precedenti possono aumentare drasticamente la quantità di informazioni inviata ai file di registrazione. Ricordarsi di ripristinare il livello di

registrazione al valore predefinito dopo aver corretto il problema, quindi ricaricare il demone appropriato affinché la configurazione abbia effetto.

1.7.3. Riferimenti

Amministrare un server Postfix può essere un compito molto complicato e potrebbe essere necessario richiedere aiuto alla comunità.

Un ottimo punto per richiedere assistenza riguardo Postfix, e per partecipare nella comunità di Ubuntu Server, è il canale IRC *#ubuntu-server* su *freenode*[4]. È anche possibile lasciare un messaggio in uno dei tanti *forum*[5].

Per informazioni dettagliate riguardo Postfix, gli sviluppatori Ubuntu consigliano il libro *The Book of Postfix*[6].

In fine, il *sito web di Postfix*[7] dispone di ottima documentazione riguardo le diverse opzioni di configurazione.

Inoltre, la pagina della *documentazione della comunità su Postfix*[8] contiene ulteriori informazioni.

---

4 http://freenode.net
5 http://www.ubuntu.com/support/community/webforums
6 http://www.postfix-book.com/
7 http://www.postfix.org/documentation.html
8 https://help.ubuntu.com/community/Postfix

2. Exim4

Exim4 è un MTA (Message Transfer Agent) sviluppato dall'Università di Cambridge per essere usato sui sistemi Unix collegati a Internet. Exim può essere installato al posto di sendmail, anche se la configurazione di exim è diversa da quella di sendmail.

2.1. Installazione

Per installare exim4, eseguire il seguente comando:

```
sudo apt-get install exim4
```

2.2. Configurazione

Per configurare Exim4, eseguire il seguente comando:

```
sudo dpkg-reconfigure exim4-config
```

Viene visualizzata l'interfaccia che consente di configurare molti dei parametri. Per esempio, in Exim4 i file di configurazione sono divisi in molti piccoli file, per averli tutti raggruppati in un unico file, è possibile farlo attraverso questa interfaccia.

Tutti i parametri che vengono configurati nell'interfaccia utente vengono archiviati nel file `/etc/exim4/update-exim4.conf`. Per riconfigurarla, è possibile eseguire nuovamente la configurazione guidata o modificare questo file usando l'editor di testo preferito. Una volta completata la configurazione, è possibile digitare il seguente comando per generare il file di configurazione principale:

```
sudo update-exim4.conf
```

Il file di configurazione principale è generato e archiviato in `/var/lib/exim4/config.autogenerated`.

Per nessun motivo modificare il file `/var/lib/exim4/config.autogenerated`. È aggiornato automaticamente ogni volta che viene eseguito il comando **update-exim4.conf**

Per avviare il demone Exim4, eseguire il seguente comando:

```
sudo service exim4 start
```

2.3. Autenticazione SMTP

Questa sezione descrive come configurare Exim4 affinché usi SMTP-AUTH con TLS e SASL.

Il primo passo è quello di creare un certificato da usare con TLS. In un terminale, digitare quanto segue:

```
sudo /usr/share/doc/exim4-base/examples/exim-gencert
```

Ora è necessario configurare Exim4 per l'utilizzo di TLS modificando il file `/etc/exim4/conf.d/main/03_exim4-config_tlsoptions` e aggiungendo quanto segue:

```
MAIN_TLS_ENABLE = yes
```

È ora necessario configurare Exim4 affinché utilizzi saslauthd per l'autenticazione. Modificare il file `/etc/exim4/conf.d/auth/30_exim4-config_examples` e de-commentare le sezioni *plain_saslauthd_server* e *login_saslauthd_server*:

```
 plain_saslauthd_server:
   driver = plaintext
   public_name = PLAIN
   server_condition = ${if saslauthd{{$auth2}{$auth3}}{1}{0}}
   server_set_id = $auth2
   server_prompts = :
   .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
   server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
   .endif
#
 login_saslauthd_server:
   driver = plaintext
   public_name = LOGIN
   server_prompts = "Username:: : Password::"
   # don't send system passwords over unencrypted connections
   server_condition = ${if saslauthd{{$auth1}{$auth2}}{1}{0}}
   server_set_id = $auth1
   .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
   server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
   .endif
```

Inoltre, per consentire a client mail esterni di connettersi al nuovo server exim, è necesario aggiungere il nuovo utente in exim usando i seguenti comandi:

```
sudo /usr/share/doc/exim4/examples/exim-adduser
```

Gli utenti dovrebbero proteggere il nuovo file password per exim con i seguenti comandi:

```
sudo chown root:Debian-exim /etc/exim4/passwd
sudo chmod 640 /etc/exim4/passwd
```

Infine, aggiornare la configurazione di Exim4 e riavviare il servizio:

```
sudo update-exim4.conf
sudo service exim4 restart
```

2.4. Configurare SASL

Questa sezione descrive come configurare saslauthd per fornire l'autenticazione per Exim4.

Per prima cosa è necessario installare il pacchetto sasl2-bin. In un terminale, digitare quando segue:

```
sudo apt-get install sasl2-bin
```

Per configurare saslauthd, modificare il file «/etc/default/saslauthd» e impostare START=no a:

```
START=yes
```

Affinché Exim4 possa usare il servizio saslauth, l'utente *Debian-exim* deve far parte del gruppo *sasl*:

```
sudo adduser Debian-exim sasl
```

Ora avviare il servizio saslauthd:

```
sudo service saslauthd start
```

Exim4 è ora configurato con il supporto a SMTP-AUTH con l'uso dell'autenticazione TLS e SASL.

2.5. Riferimenti

- Per maggiori informazioni, consultare *exim.org*[9].
- È anche disponibile un *libro su Exim4*[10].
- Un'altra risorsa è la pagina della *documentazione della comunità su Exim4*[11].

[9] http://www.exim.org/
[10] http://www.uit.co.uk/content/exim-smtp-mail-server
[11] https://help.ubuntu.com/community/Exim4

3. Server Dovecot

Dovecot è un Mail Delivery Agent progettato per garantire la sicurezza. Supporta la maggior parte dei formati di caselle di posta: mbox o maildir. Questa sezione espone come configurarlo come server imap o pop3.

3.1. Installazione

Per installare dovecot, in un terminale, digitare:

```
sudo apt-get install dovecot-imapd dovecot-pop3d
```

3.2. Configurazione

Per configurare dovecot è possibile modificare il file `/etc/dovecot/dovecot.conf`. È possibile scegliere il protocollo da usare, che può essere pop3, pop3s (pop3 sicuro), imap and imaps (imap sicuro). Una descrizione di questi protocolli va oltre lo scopo di questa guida. Per maggiori informazioni, fare riferimento agli articoli su Wikipedia relativi a *POP3*[12] e *IMAP*[13].

IMAPS e POP3S sono più sicuri dei semplici IMAP e POP3 poiché utilizzano la cifratura SSL per connettersi. Una volta scelto il protocollo, modificare la seguente riga nel file `/etc/dovecot/dovecot.conf`:

```
protocols = pop3 pop3s imap imaps
```

Quindi, scegliere la mailbox che si desidera usare. Dovecot supporta i formati **maildir** e **mbox**, che sono i formati di mailbox più comunemente usati. Entrambi hanno i propri vantaggi, discussi sul *sito web di Dovecot*[14].

Una volta scelta la tipologia della casella di posta, modificare il file `/etc/dovecot/dovecot.conf` e cambiare la seguente riga:

```
mail_location = maildir:~/Maildir # (per maildir)
oppure
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (per mbox)
```

È necessario configurare l'MTA (Mail Transport Agent) per trasferire le mail ricevute in questo tipo di casella di posta se è differente da quella impostata.

Una volta configurato, riavviare il demone dovecot per provare le impostazioni:

12 http://en.wikipedia.org/wiki/POP3
13 http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol
14 http://wiki.dovecot.org/MailboxFormat

```
sudo service dovecot restart
```

Se è stato abilitato imap o pop3, è possibile provare a eseguire l'accesso con i comandi **telnet localhost pop3** o **telnet localhost imap2**. Se viene visualizzata una schermata simile alla seguente, l'installazione è stata eseguita con successo:

```
telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

3.3. Configurazione di Dovecot SSL

Per configurare dovecot affinché utilizzi SSL, è possibile modificare il file `/etc/dovecot/dovecot.conf` e cambiare le seguenti righe:

```
ssl_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
ssl_key_file = /etc/ssl/private/ssl-cert-snakeoil.key
ssl_disable = no
disable_plaintext_auth = no
```

È possibile ottenere il certificato SSL da un'entità di certificazione oppure è possibile creare il proprio certificato auto-firmato. Quest'ultima opzione è valida per le email, dato che i client SMPT solitamente non danno grossi problemi a riguardo. Per maggiori informazioni su come creare un certificato SSL, consultare *Sezione 5, «Certificati» [172]*. Una volta creato, sono disponibili una chiave e un certificato sotto forma di file, copiarli nella posizione puntata all'interno del file `/etc/dovecot/dovecot.conf`.

3.4. Configurazione del firewall per un server email

Per accedere al server mail da un altro computer, è necessario configurare il firewall affinché consenta i collegamenti al server sulle porte necessarie.

- IMAP - 143
- IMAPS - 993
- POP3 - 110
- POP3S - 995

3.5. Riferimenti

- Per maggiori informazioni, consultare il *sito web di Dovecot*[15].
- Consultare anche la pagina della *documentazione della comunità su Dovecot*[16] per ulteriori dettagli.

[15] http://www.dovecot.org/
[16] https://help.ubuntu.com/community/Dovecot

4. Mailman

Mailman è un programma open source per la gestione di discussioni elettroniche e newsletter. Molte mailing list open source (incluse tutte le mailing list di *Ubuntu*[17]) utilizzano Mailman come software. È molto potente e facile da installare.

4.1. Installazione

Mailman dispone in un'interfaccia web sia per gli amministratori che per gli utenti, utilizzando un server mail esterno per inviare e ricevere le email e si integra perfettamente con i seguenti server mail:

- Postfix
- Exim
- Sendmail
- Qmail

Viene descritto come installare Mailman, il server web Apache e il server mail Postfix o Exim. Per installare Mailman con un server mail diverso, fare riferimento alla sezione «Riferimenti».

È necessario installare solamente un server mail e Postfix è il Mail Transfer Agent predefinito di Ubuntu.

4.1.1. Apache2

Per i dettagli relativi all'installazione di Apache2, consultare *Sezione 1.1, «Installazione» [188]*.

4.1.2. Postfix

Per le istruzioni su come installare e configurare Postfix, consultare *Sezione 1, «Postfix» [236]*

4.1.3. Exim4

Per installare Exim4, consultare *Sezione 2, «Exim4» [243]*.

Una volta installato exim4, i file di configurazione sono salvati nella directory `/etc/exim4`. In Ubuntu, per impostazione predefinita, i file di configurazione di exim4 sono divisi tra vari file, ma è possibile cambiare questo comportamento modificando la seguente variabile nel file `/etc/exim4/update-exim4.conf`:

```
dc_use_split_config='true'
```

4.1.4. Mailman

Per installare Mailman, in un terminale, digitare il seguente comando:

[17] http://lists.ubuntu.com

```
sudo apt-get install mailman
```

Questo copia i file di installazione nella directory /var/lib/mailman, gli script CGI nella directory /usr/lib/cgi-bin/mailman, crea l'utente *list* e il gruppo *list*. Il proprietario del processo mailman sarà l'utente creato.

4.2. Configurazione

Questa sezione ha come presupposto l'avvenuta installazione di mailman, apache2 e di postfix o exim4. Ora è solo necessario configurarle.

4.2.1. Apache2

Un file di esempio di Apache è disponibile con Mailman ed è localizzato in `/etc/mailman/apache.conf`. Affinché Apache possa utilizzare il file di configurazione è necessario copiarlo in `/etc/apache2/sites-available`:

```
sudo cp /etc/mailman/apache.conf /etc/apache2/sites-available/mailman.conf
```

In questo modo verrà configurato un nuovo *VirtualHost* per il sito di amministrazione di Mailman. Ora è necessario abilitare la configurazione e riavviare Apache:

```
sudo a2ensite mailman.conf
sudo service apache2 restart
```

Mailman utilizza apache2 per eseguire gli script CGI. Gli script CGI di mailman sono installati all'interno della directory /usr/lib/cgi-bin/mailman e l'URL di mailman risulta quindi «http://hostname/cgi-bin/mailman/». È possibile apportare cambiamenti al file `/etc/apache2/sites-available/mailman.conf` per modificarne il comportamento.

4.2.2. Postfix

Per l'integrazione di Postfix, verrà associato il dominio «lists.example.com» con le seguenti mailing list. Sostituire *lists.example.com* con il proprio dominio.

È possibile usare il comando postconf per aggiungere la configurazione necessaria in `/etc/postfix/main.cf`:

```
sudo postconf -e 'relay_domains = lists.example.com'
sudo postconf -e 'transport_maps = hash:/etc/postfix/transport'
sudo postconf -e 'mailman_destination_recipient_limit = 1'
```

Controllare che in `/etc/postfix/master.cf` sia presente quanto segue:

```
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
```

```
  ${nexthop} ${user}
```

Invoca lo script *postfix-to-mailman.py* quando viene ricevuta una mail in una lista.

Associare il dominio «lists.example.com» a Mailman con la mappa dei metodi «transport». Modificare il file `/etc/postfix/transport`:

```
lists.example.com      mailman:
```

Ora è necessario far generare a Postfix la mappa «transport» digitando, in un terminale:

```
sudo postmap -v /etc/postfix/transport
```

Riavviare Postfix per abilitare le nuove configurazioni:

```
sudo service postfix restart
```

4.2.3. Exim4

Una volta installato Exim4, è possibile avviare il server Exim digitando, in un terminale, il seguente comando:

```
sudo service exim4 start
```

Affinché mailman funzioni con Exim4, è necessario configurare Exim4. Come già spiegato, Exim4 utilizza molteplici file di configurazione di diverse tipologia (per maggiori informazioni, fare riferimento al *sito web di Exim*[18]). Per poter eseguire mailman, è necessario aggiungere un nuovo file di configurazione alle seguenti tipologie di configurazione:

- Main
- Transport
- Router

Exim quindi crea un file di configurazione principale ordinando tutti i file di configurazione: l'ordine di questi file è molto importante.

4.2.4. Main

Tutti i file di configurazione appartenenti al tipo main sono archiviati nella directory `/etc/exim4/conf.d/main/`. È possibile aggiungere il seguente contenuto a un nuovo file di configurazione chiamato `04_exim4-config_mailman`:

```
# start
# Home dir for your Mailman installation -- aka Mailman's prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman"
```

[18] http://www.exim.org

```
# This is normally the same as ~mailman
MM_HOME=/var/lib/mailman
#
# User and group for Mailman, should match your --with-mail-gid
# switch to Mailman's configure script. Value is normally "mailman"
MM_UID=list
MM_GID=list
#
# Domains that your lists are in - colon separated list
# you may wish to add these into local_domains as well
domainlist mm_domains=hostname.com
#
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
#
# These values are derived from the ones above and should not need
# editing unless you have munged your mailman installation
#
# The path of the Mailman mail wrapper script
MM_WRAP=MM_HOME/mail/mailman
#
# The path of the list config file (used as a required file when
# verifying list addresses)
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck
# end
```

4.2.5. Transport

Tutti i file di configurazione appartenenti al tipo transport sono archiviati nella directory `/etc/exim4/conf.d/transport/`. È possibile aggiungere il seguente contenuto a un nuovo file di configurazione chiamato `40_exim4-config_mailman`:

```
  mailman_transport:
   driver = pipe
   command = MM_WRAP \
               '${if def:local_part_suffix \
                    {${sg{$local_part_suffix}{-(\\w+)(\\+.*)?}{\$1}}} \
                    {post}}' \
               $local_part
    current_directory = MM_HOME
    home_directory = MM_HOME
    user = MM_UID
    group = MM_GID
```

4.2.6. Router

Tutti i file di configurazione appartenenti al tipo router sono archiviati nella directory `/etc/exim4/conf.d/router/`. È possibile aggiungere il seguente contenuto a un nuovo file di configurazione chiamato `101_exim4-config_mailman`:

```
  mailman_router:
```

```
driver = accept
require_files = MM_HOME/lists/$local_part/config.pck
local_part_suffix_optional
local_part_suffix = -bounces : -bounces+* : \
                    -confirm+* : -join : -leave : \
                    -owner : -request : -admin
transport = mailman_transport
```

L'ordine dei file di configurazione main e transport può essere qualsiasi. L'ordine dei file di configurazione del tipo router deve essere lo stesso. Questo particolare file deve apparire prima del file `200_exim4-config_primary`. Questi file contengono le stesse informazioni, ma il primo ha la precedenza. Per maggiori informazioni fare riferimento alla sezione «Riferimenti».

4.2.7. Mailman

Una volta installato mailman, è possibile avviarlo usando il seguente comando:

```
sudo service mailman start
```

Creare quindi la mailing list predefinita. Per crearla, eseguire il seguente comando:

```
sudo /usr/sbin/newlist mailman
```

```
Enter the email address of the person running the list: bhuvan at ubuntu.com
Initial mailman password:
To finish creating your mailing list, you must edit your /etc/aliases (or
equivalent) file by adding the following lines, and possibly running the
`newaliases' program:

## mailman mailing list
mailman: "|/var/lib/mailman/mail/mailman post mailman"
mailman-admin: "|/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces: "|/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm: "|/var/lib/mailman/mail/mailman confirm mailman"
mailman-join: "|/var/lib/mailman/mail/mailman join mailman"
mailman-leave: "|/var/lib/mailman/mail/mailman leave mailman"
mailman-owner: "|/var/lib/mailman/mail/mailman owner mailman"
mailman-request: "|/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe: "|/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe: "|/var/lib/mailman/mail/mailman unsubscribe mailman"

Hit enter to notify mailman owner..

#
```

Postfix o Exim4 sono stati configurati per riconoscere tutte le email di mailman ed è ora obbligatorio creare le nuove voci in `etc/aliases`. Se sono state apportate modifiche ai file di configurazione, assicurarsi di riavviare tali servizi prima di continuare.

Exim4 non utilizza gli alias precedenti per inoltrare le mail a Mailman dato che usa un approccio di tipo *discover*. Per eliminare gli alias quando viene creato l'elenco, è possibile aggiungere la riga *MTA=None* nel file di configurazione di Mailman `/etc/mailman/mm_cfg.py`.

4.3. Amministrazione

Si assume che sia stata fatta un'installazione di base. Gli script cgi di mailman si trovano nella directory /usr/lib/cgi-bin/mailman/. Mailman fornisce uno strumento di amministrazione basato sul web, per accedere alla relativa pagina, aprire con il browser il seguente url:

http://hostname/cgi-bin/mailman/admin

La mailing list di base, *mailman*, comparirà in questa schermata. Facendo clic sul nome della mailing list, verrà richiesta la password di autenticazione. Se viene inserita la password corretta sarà possibile modificare le preferenze di amministrazione di questa mailing list. È possibile creare una nuova mailing list usando l'utilità a riga di comando (**/usr/sbin/newlist**). In alternativa, è possibile creare una nuova mailing list usando l'interfaccia web.

4.4. Utenti

Mailman fornisce un'interfaccia web per gli utenti. Per accedere a questa pagina, indirizzare il browser web al seguente URL:

http://hostname/cgi-bin/mailman/listinfo

La mailing list predefinita, *mailman*, compare a schermo. Facendo clic sul nome, viene presentato il modulo di iscrizione. È possibile inserire il proprio indirizzo email, il nome (opzionale) e la password per completare l'iscrizione. Viene così inviata una email di invito all'indirizzo specificato. È possibile seguire le istruzioni contenute nell'email per completare l'iscrizione.

4.5. Riferimenti

GNU Mailman - Manuale di installazione[19]

HOWTO - Using Exim 4 and Mailman 2.1 together[20]

Consultare anche la pagina della *documentazione della comunità su Mailman*[21].

[19] http://www.list.org/mailman-install/index.html
[20] http://www.exim.org/howto/mailman21.html
[21] https://help.ubuntu.com/community/Mailman

5. Filtrare le email

Uno dei più grandi problemi oggigiorno con le email è lo Unsolicited Bulk Email (UBE). Conosciuto anche come SPAM, questi messaggi possono essere virus e altre forme di malware. Secondi alcuni rapporti, questi messaggi compongono la maggior parte del traffico di email su Internet.

Questa sezione descrive come integrare Amavisd-new, Spamassassin, e ClamAV con il Mail Transport Agent (MTA) Postfix. Postfix può anche verificare la validità delle email facendole analizzare da filtri esterni, che in certi casi possono determinare se un messaggio è indesiderato senza doverlo elaborare con applicazioni che richiedono più risorse. Due filtri d'uso comune sono opendkim e python-policyd-spf.

- Amavisd-new è un «wrapper» che può chiamare qualsiasi programma di filtraggio per rilevare la posta indesiderata, virus, ecc...
- Spamassassin utilizza moti meccanismi diversi per filtrare le email in base al contenuto del messaggio.
- ClamAV è un antivirus open source.
- opendkim implementa un Sendmail Mail Filter (Milter) per lo standard DomainKeys Identified Mail (DKIM).
- python-policyd-spf abilita il controllo Sender Policy Framework (SPF) con Postfix.

Il processo di elaborazione è il seguente:

- Un messaggio email viene accettato da Postfix.
- Il messaggio è elaborato dai filtri esterni, in questo caso opendkim e python-policyd-spf.
- Amavisd-new quindi elabora il messaggio.
- ClamAV analizza il messaggio. Se contiene un virus, Postfix rifiuta il messaggio.
- I messaggi puliti vengono poi analizzati da Spamassassin per verificare che non sia indesiderato. Spamassassin aggiunge quindi una riga X-Header per consentire ad Amavisd-new di analizzare ulteriormente il messaggio.

Per esempio, se un messaggio ha un punteggio spam di oltre 50, questo può essere scartato automaticamente senza nemmeno farlo arrivare al ricevente. Un altro metodo per gestire i messaggi con una segnalazione, è quello di lasciarli arrivare al Mail User Agent (MUA) consentendo all'utente di gestirli come meglio crede.

5.1. Installazione

Per maggiori informazioni sull'installazione e la configurazione di Postfix, consultare *Sezione 1, «Postfix» [236]*.

Per installare le restanti applicazioni, in un terminale, digitare:

```
sudo apt-get install amavisd-new spamassassin clamav-daemon
sudo apt-get install opendkim postfix-policyd-spf-python
```

Esistono dei pacchetti opzionali che si integrano con Spamassassin per rilevare più efficientemente la posta indesiderata:

```
sudo apt-get install pyzor razor
```

Oltre alle applicazioni per il filtraggio, sono necessarie le utilità di compressione per elaborare alcuni allegati delle email.

```
sudo apt-get install arj cabextract cpio lha nomarch pax rar unrar unzip zip
```

Se non è possibile trovare alcuni pacchetti, controllare che il repository *multiverse* sia abilitato `/etc/apt/sources.list`

Se vengono effettuate modifiche al file, assicurarsi di eseguire il comando **sudo apt-get update** prima di tentare nuovamente l'installazione.

5.2. Configurazione

Ora è necessario configurare il tutto affinché i programmi funzionino assieme e vengano filtrate le email.

5.2.1. ClamAV

Il comportamento predefinito di ClamAV soddisferà le proprie necessità. Per le altre opzioni di ClamAV, controllare i file di configurazioni presenti in `/etc/clamav`.

Aggiungere l'utente *clamav* al gruppo *amavis* affinché Amavisd-new possa avere accesso per analizzare i file:

```
sudo adduser clamav amavis
sudo adduser amavis clamav
```

5.2.2. Spamassassin

Spamassassin rileva automaticamente i componenti opzionali e ne fa uso se sono presenti. Ciò significa che non c'è alcuna necessità di configurare pyzor e razor.

Modificare `/etc/default/spamassassin` per attivare il demone Spamassassin daemon. Cambiare *ENABLED=0* in:

```
ENABLED=1
```

Ora avviare il demone:

```
sudo service spamassassin start
```

5.2.3. Amavisd-new

Per prima cosa, attivare il rilevamento spam e antivirus in Amavisd-new modificando `/etc/amavis/conf.d/15-content_filter_mode`:

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Uncomment the two lines below to enable it
#

@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);


#
# Default SPAM checking mode
# Uncomment the two lines below to enable it
#

@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # insure a defined return
```

rifiutare lo spam e rinviarlo al mittente può essere una cattiva idea, dato che l'indirizzo solitamente è fasullo. Modificare quindi `/etc/amavis/conf.d/20-debian_defaults` per impostare *$final_spam_destiny* a «D_DISCARD» piuttosto che «D_BOUNCE»:

```
$final_spam_destiny       = D_DISCARD;
```

Per indicare più messaggi come indesiderati, è possibile utilizzare anche questa opzione:

```
$sa_tag_level_deflt = -999; # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.0; # add 'spam detected' headers at that level
$sa_kill_level_deflt = 21.0; # triggers spam evasive actions
$sa_dsn_cutoff_level = 4; # spam level beyond which a DSN is not sent
```

Se il *nome host* del server è diverso dal record MX del dominio è necessario impostare manualmente l'opzione *$myhostname*. Inoltre, se il server riceve email da diversi domini, è necessario personalizzare l'opzione *@local_domains_acl*. Modificare il file `/etc/amavis/conf.d/50-user`:

```
$myhostname = 'mail.example.com';
@local_domains_acl = ( "example.com", "example.org" );
```

Se è necessario servirsi di diversi domini, inserire quanto segue in `/etc/amavis/conf.d/50-user`

```
@local_domains_acl = qw(.);
```

Una volta configurato, Amavisd-new deve essere riavviato:

```
sudo service amavis restart
```

5.2.3.1. Whitelist DKIM

Amavisd-new può essere configurato per inserire automaticamente in una *whitelist* gli indirizzi da domini dotati di «Domain Keys» valide. Nel file `/etc/amavis/conf.d/40-policy_banks` sono disponibili alcuni domini preconfigurati.

L'aggiunta di un dominio nella whitelist è possibile in diversi modi:

- *'example.com' => 'WHITELIST',*: inserisce nella whitelist qualsiasi indirizzo dal dominio «example.com».
- *'.example.com' => 'WHITELIST',*: inserisce nella whitelist qualsiasi indirizzo da qualsiasi *sotto dominio* di «example.com» con una firma valida.
- *'.example.com/@example.com' => 'WHITELIST',*: inserisce nella whitelist i sotto domini di «example.com» che utilizzano una firma del dominio superiore *example.com*.
- *'./@example.com' => 'WHITELIST',*: inserisce gli indirizzi con una firma valida da «example.com». Molto usato dai gruppi di discussione in cui vengono firmati i messaggi.

Un dominio può anche avere molteplici configurazioni di whitelist; una volta modificato il file, riavviare amavisd-new:

```
sudo service amavis restart
```

In questo contesto, una volta aggiunto un dominio alla whitelist, il messaggio non verrà più filtrato dall'anti-virus o dal filtro anti-spam. Questo potrebbe essere o meno un comportamento indesiderato per un dominio.

5.2.4. Postfix

Per l'integrazione con Postfix, in un terminale, digitare quanto segue:

```
sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
```

Ora modificare il file `/etc/postfix/master.cf` e aggiungere quanto segue alla fine:

```
smtp-amavis     unix    -       -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20

127.0.0.1:10025 inet    n       -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

Aggiungere anche le seguenti righe dopo il servizio di trasporto «*pickup*»:

```
         -o content_filter=
         -o receive_override_options=no_header_body_checks
```

In questo modo si eviteranno i messaggi generati per segnalare lo spam che viene classificato come spam.

Infine riavviare Postfix:

```
sudo service postfix restart
```

Il filtraggio sul contenuto per lo spam e il rilevamento di virus sono ora abilitati.

5.2.5. Amavisd-new e Spamassassin

Integrando Amavisd-new con Spamassassin, se si sceglie di disabilitare i filtri bayesiani modificando `/etc/spamassassin/local.cf` e usando cron per aggiornare le regole durante la notte, il risultato può essere una situazione in cui una grande quantità di errori viene inviata all'utente *amavis* a causa dell'attività di amavisd-new cron.

Ci sono diversi modi per gestire questa situazione:

- Configurare il MDA per filtrare i messaggi da nascondere.

- Modificare `/usr/sbin/amavisd-new-cronjob` per verificare la presenza di *use_bayes 0*. Per esempio, modificare `/usr/sbin/amavisd-new-cronjob` e aggiungere quanto segue all'inizio, prima dell'istruzione *test*:

```
egrep -q "^[ \t]*use_bayes[ \t]*0" /etc/spamassassin/local.cf && exit 0
```

5.3. Test

Per prima cosa, verificare che Amavisd-new SMTP sia in ascolto:

```
telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
^]
```

Nell'intestazione dei messaggi che passano attraverso il filtraggio del contenuto, dovrebbe essere visibile:

```
X-Spam-Level:
X-Virus-Scanned: Debian amavisd-new at example.com
X-Spam-Status: No, hits=-2.3 tagged_above=-1000.0 required=5.0 tests=AWL, BAYES_00
X-Spam-Level:
```

L'output potrebbe variare, ma l'aspetto importante è la presenza delle voci *X-Virus-Scanned* e *X-Spam-Status*.

5.4. Risoluzione problemi

Il miglior metodo per comprendere cosa non funzioni correttamente è controllare i file di registro.

- Per istruzioni sulle registrazioni di Postfix, consultare *Sezione 1.7, «Risoluzione problemi» [240]*.
- Amavisd-new fa uso di Syslog per inviare i messaggi verso `/var/log/mail.log`. Il livello di dettaglio può essere aumentato aggiungendo l'opzione *$log_level* in `/etc/amavis/conf.d/50-user` e impostando il valore da 1 a 5.

```
$log_level = 2;
```

Quando il livello dei messaggi di registro di Amavisd-new viene aumentato, viene aumentato automaticamente anche quello di Spamassassin.

- Il livello di messaggi di ClamAV può invece essere aumentato modificando il file `/etc/clamav/clamd.conf` e impostando la seguente opzione:

```
LogVerbose true
```

ClamAV, in modo predefinito, invia i messaggi verso `/var/log/clamav/clamav.log`.

Dopo aver cambiato le impostazioni di registrazione di un'applicazione, ricordarsi di riavviare il servizio. Una volta risolto il problema, è buona norma ripristinare il livello di registrazioni originale.

5.5. Riferimenti

Per maggiori informazioni sul filtraggio mail, consultare i seguenti indirizzi:

- *Documentazione di Amavisd-new*[22]
- *Documentazione ClamAV*[23] e *ClamAV*[24]
- *Wiki di Spamassassin*[25]
- *Sito web di Pyzor*[26]
- *Sito web di Razor*[27]
- *DKIM.org*[28]
- *Postfix Amavis New*[29]

È possibile anche porre le proprie domande nel canale IRC *#ubuntu-server* su *freenode*[30].

[22] http://www.ijs.si/software/amavisd/amavisd-new-docs.html
[23] http://www.clamav.net/doc/latest/html/
[24] http://wiki.clamav.net/Main/WebHome
[25] http://wiki.apache.org/spamassassin/
[26] http://sourceforge.net/apps/trac/pyzor/
[27] http://razor.sourceforge.net/
[28] http://dkim.org/
[29] https://help.ubuntu.com/community/PostfixAmavisNew
[30] http://freenode.net

Capitolo 16. Applicazioni per conversazioni

1. Panoramica

In questa sezione viene discusso come installare e configurare un server IRC (ircd-irc2) e come installare e configurare Jabber, un server di messaggistica istantanea.

2. Server IRC

Nei repository di Ubuntu sono disponibili molti server Internet Relay Chat, ma in questa sezione viene descritto come installare e configurare il server IRC ircd-irc2.

2.1. Installazione

Per installare ircd-irc2, eseguire il seguente comando in un terminale:

```
sudo apt-get install ircd-irc2
```

I file di configurazione sono presenti nella directory `/etc/ircd`, i documenti nella directory `/usr/share/doc/ircd-irc2`.

2.2. Configurazione

Le impostazioni IRC possono essere svolte nel file di configurazione `/etc/ircd/ircd.conf`, dove è possibile impostare il nome host IRC modificando la seguente riga:

```
M:irc.localhost::Debian ircd default configuration::000A
```

Assicurarsi di aggiungere gli alias DNS per il nome host IRC. Per esempio, se il nome host IRC è irc.example.net, assicurarsi che irc.example.net possa essere risolto dal proprio DNS. Il nome host IRC non dovrebbe essere lo stesso del nome host.

I dettagli dell'amministratore possono essere configurati modificando la seguente riga:

```
A:Organization, IRC dept.:Daemon <ircd@example.irc.org>:Client Server::IRCnet:
```

Per configurare le porte IRC da ascoltare, per configurare le credenziali di Operator o l'autenticazione lato client, è necessario aggiungere delle specifiche righe nel file di configurazione. Per maggiori informazioni, fare riferimento al file di configurazione di esempio `/usr/share/doc/ircd-irc2/ircd.conf.example.gz`.

Il messaggio (banner) IRC da visualizzare nei client IRC, quando gli utenti si connettono al server, può essere impostato nel file `/etc/ircd/ircd.motd`.

Una volta apportate le necessarie modifiche al file di configurazione, riavviare il server IRC tramite il seguente comando:

```
sudo service ircd-irc2 restart
```

2.3. Riferimenti

Potrebbe essere interessante controllare anche altri server IRC disponibili nei repository Ubuntu come ircd-ircu e ircd-hybrid.

- Per maggiori informazioni riguardo il server IRC, consultare le *IRCD FAQ*[1].

[1] http://www.irc.org/tech_docs/ircnet/faq.html

3. Server di messaggistica istantanea Jabber

Jabber è un protocollo di messaggistica molto diffuso, basato su XMPP, uno standard aperto per la messaggistica istantanea e usato da molte applicazioni. Questa sezione espone come configurare un server *Jabberd 2* in una rete locale. La configurazione può anche essere adattata per fornire servizi di messaggistica agli utenti attraverso Internet.

3.1. Installazione

Per installare jabberd2, in un terminale digitare:

```
sudo apt-get install jabberd2
```

3.2. Configurazione

Verranno usati un paio di file XML per configurare jabberd2 affinché utilizzi l'autenticazione utente *Berkeley DB*, una semplice forma di autenticazione. È comunque possibile configurare jabberd2 per l'uso di LDAP, MySQL, PostgreSQL, ecc... per l'autenticazione utente.

Aprire il file `/etc/jabberd2/sm.xml` e alla riga:

```
<id>jabber.example.com</id>
```

Sostituire *jabber.example.com* con il nome host, o altro identificativo, del proprio server.

Nella sezione <storage>, modificare <driver> in:

```
<driver>db</driver>
```

Modificare il file `/etc/jabberd2/c2s.xml` e nella sezione <*local*> cambiare:

```
<id>jabber.example.com</id>
```

Nella sezione <authreg> sistemare la sezione <module> in

```
<module>db</module>
```

Riavviare jabberd2 per abilitare le nuove impostazioni:

```
sudo service jabberd2 restart
```

Dovrebbe quindi essere possibile connettersi al server utilizzando un client Jabber come Empathy.

Il vantaggio nell'uso di Berkeley DB per i dati utenti consiste nella bassa manutenzione necessaria una volta configurato. Per avere un maggiore controllo sugli account utente e le credenziali di autenticazione, è consigliato usare un altro metodo di autenticazione.

3.3. Riferimenti

- Il *sito web di Jabberd2*[2] contiene molte informazioni sulla configurazione di Jabberd2.
- Per ulteriori opzioni sull'applicazione, consultare *Guida all'installazione di Jabberd2*[3].
- Ulteriori informazioni sono disponibili nella *documentazione online*[4].

[2] http://codex.xiaoka.com/wiki/jabberd2:start
[3] http://www.jabberdoc.org/
[4] https://help.ubuntu.com/community/SettingUpJabberServer

Capitolo 17. Sistemi per il controllo della versione

Il controllo della versione è l'arte della gestione dell'evolversi delle informazioni. È stato a lungo uno strumento critico per i programmatori, che spendono il loro tempo apportando piccole modifiche al software per poi cancellarle il giorno seguente. Ma l'utilità del software per il controllo della versione va oltre il mondo dello sviluppo di programmi. Ovunque si incontrino persone che utilizzino il computer per gestire informazioni in continuo cambiamento c'è posto per il controllo della versione.

1. Bazaar

Bazaar è un nuovo sistema di controllo della versione sponsorizzato da Canonical, la società commerciale dietro Ubuntu. Diversamente da Subversion e CVS che supportano solamente un modello centralizzato di repository, Bazaar supporta anche un *controllo distribuito della versione,* consentendo alle persone di collaborare più efficientemente. In particolare, Bazaar è progettato per massimizzare il livello di partecipazione della comunità nei progetti open source.

1.1. Installazione

Per installare bzr, in un terminale, digitare:

```
sudo apt-get install bzr
```

1.2. Configurazione

Per introdursi a bzr, usare il comandi *whoami*:

```
$ bzr whoami 'Mario Rossi <mario.rossi@ubuntu.com>'
```

1.3. Imparare a usare Bazaar

La documentazione fornita con Bazaar è installata in /usr/share/doc/bzr/html, il tutorial è un buon punto di partenza. Il comando bzr è dotato di un sistema di aiuto integrato:

```
$ bzr help
```

Per avere maggiori informazioni riguardo il comando *foo*:

```
$ bzr help foo
```

1.4. Integrazione con Launchpad

Anche se è altamente utilizzabile come strumento dedicato, Bazaar è dotato di un'ottima integrazione con *Launchpad*[1], il sistema di sviluppo collaborativo utilizzato da Canonical, e altre comunità di progetti open source, per la gestione di Ubuntu. Per informazioni su come Bazaar possa essere usato con Launchpad per la collaborazione nei progetti open source, consultare *http://bazaar-vcs.org/LaunchpadIntegration*[2].

---

[1] https://launchpad.net/

[2] http://bazaar-vcs.org/LaunchpadIntegration/

2. Subversion

Subversion è un software open source per il controllo della versione. Utilizzando Subversion è possibile registrare la storia del codice sorgente e dei documenti. È in grado di gestire l'evolversi di file e directory nel tempo. Nel repository centrale viene posizionato un albero di tutti i file. Il repository è come un server di file, tranne per il fatto che si ricorda qualsiasi cambiamento apportato.

2.1. Installazione

Per accedere al repository di Subversion utilizzando il protocollo HTTP, è necessario installare e configurare un server web come Apache2, che funziona molto bene con Subversion. Fare riferimento alla sottosezione HTTP della sezione relativa ad Apache2 per installare e configurare un certificato digitale.

Per installare Subversion, in un terminale, digitare:

```
sudo apt-get install subversion libapache2-svn
```

2.2. Configurazione del server

I passi seguenti presumono siano stati installati i pacchetti elencati in precedenza. Questa sezione descrive come creare un repository con Subversion e come accedere al progetto.

2.2.1. Creare un repository con Subversion

Un repository può essere creato con il seguente comando:

```
svnadmin create /posizione/del/repository/project
```

2.2.2. Importare i file

Una volta creato il repository è possibile *import*arvi file. Per importare una directory, digitare ciò che segue al prompt del terminale:

```
svn import /percorso/della/directory/da/importare file:///percorso/del/repository/
```

2.3. Metodi di accesso

È possibile accedere (checkout) ai repository Subversion in diversi modi, sul disco locale o attraverso diversi protocolli di rete. La posizione di un repository, comunque, è sempre un URL. La tabella illustra come i diversi schemi URL vengono mappati ai diversi metodi di accesso.

Tabella 17.1. Metodi di accesso

Schema	Metodo di accesso
file://	Accesso diretto al repository (sul disco locale)

Schema	**Metodo di accesso**
http://	Accesso attraverso il protocollo WebDAV al server web Apache2 di Subversion
https://	Come http://, ma con cifratura SSL
svn://	Accesso attraverso un protocollo personalizzato a un server svnserve
svn+ssh://	Come svn://, ma attraverso un tunnel SSH

In questa sezione viene descritto come configurare Subversion per tutti questi metodi. Saranno descritti solo gli elementi basilari. Per maggiori informazioni, fare riferimento al *libro di svn*[3].

2.3.1. Accesso diretto al repository (file://)

Questo è il metodo di accesso più semplice. Non necessita di alcun server di Subversion in esecuzione e serve per accedere a Subversion dalla stessa macchina in cui è in esecuzione. La sintassi del comando è la seguente:

```
svn co file:///percorso/del/repository/progetto
```

o

```
svn co file://localhost/percorso/del/repository/progetto
```

Se non viene specificato l'host, è necessario utilizzare tre slash (///), due per il protocollo (in questo caso file) e uno è lo slash iniziale del percorso. Se viene specificato l'host, utilizzare due slash (//).

I permessi di accesso al repository dipendono dai permessi impostati nel file system. Se l'utente possiede i permessi di scrittura e lettura, allora potrà eseguire checkout e commit al repository.

2.3.2. Accesso con il protocollo WebDAV (http://)

Per accedere al repository di Subversion utilizzando il protocollo WebDAV, è necessario configurare il server web Apache2. Aggiungere quanto segue fra gli elementi *<VirtualHost>* e *</VirtualHost>* in `/etc/apache2/sites-available/default`, o altro file VirtualHost:

```
<Location /svn>
 DAV svn
 SVNPath /home/svn
 AuthType Basic
 AuthName "Your repository name"
 AuthUserFile /etc/subversion/passwd
 Require valid-user
</Location>
```

[3] http://svnbook.red-bean.com/

L'esempio di configurazione precedente assume che i repository di Subversion siano creati nella directory `/home/svn/` usando il comando **svnadmin**. Sono accessibili usando l'indirizzo **http://NOME_HOST/svn/NOME_REPOSITORY**.

Per importare o eseguire il «commit» di file nel proprio repository Subversion via HTTP, il repository deve essere di proprietà dell'utente del servizio HTTP. Nei sistemi Ubuntu, solitamente, l'utente del servizio HTTP è **www-data**. Per cambiare il proprietario dei file del repository, digitare il comando seguente in un terminale:

```
sudo chown -R www-data:www-data /percorso/al/repository
```

Modificando il proprietario del repository come **www-data** non sarà più possibile importare o eseguire il «commit» di file nel repository attraverso il comando **svn import file:///** come un qualsiasi utente, ma solo come **www-data**.

Creare il file `/etc/subversion/passwd` che conterrà i dettagli di autenticazione utente. Per creare un file, eseguire il seguente comando al prompt dei comandi (viene creato il file e aggiunto il primo utente):

```
sudo htpasswd -c /etc/subversion/passwd nome_utente
```

Per aggiungere ulteriori utenti, omettere l'opzione «*-c*» poiché questa opzione sostituisce i vecchio file. Usare invece questa forma:

```
sudo htpasswd /etc/subversion/passwd nome_utente
```

Verrà richiesta la password. Una volta inserita, l'utente viene aggiunto al file. Ora, per accedere al repository, digitare:

```
svn co http://servername/svn
```

La password viene trasmessa come testo in chiaro. Per evitare attacchi di tipo «password snooping», è necessario utilizzare la cifratura SSL. Per maggiori informazioni fare riferimento alla sezione successiva.

2.3.3. Accesso con protocollo WebDAV protetto da cifratura SSL (https://)

Accedere a un repository Subversion attraverso il protocollo WebDAV con cifratura SSL (https://) è simile a http://, l'unica differenza sta nel dover installare e configurare il certificato digitale nel server web Apache. Per usare SSL con Subversion, aggiungere la precedente configurazione di Apache2 al file `/etc/apache2/sites-available/default-ssl`. Per maggiori informazioni su come configurare Apache2 con SSL, consultare *Sezione 1.3, «Configurazione HTTPS» [194]*.

È possibile installare un certificato digitale emesso da un'autorità certificante o in alternativa è possibile usare un certificato auto-firmato.

I passi seguenti hanno come presupposto l'installazione di un certificato digitale all'interno del server web Apache2. Per accedere a un repository Subversion, fare riferimento alla sezione precedente. I metodi di accesso sono esattamente gli stessi tranne per il protocollo, in quanto è necessario utilizzare https://.

2.3.4. Accesso con il protocollo personalizzato (svn://)

Una volta creato il repository è possibile configurare il controllo degli accessi modificando il file `/path/to/repos/project/conf/svnserve.conf`. Per esempio, per impostare l'autenticazione, togliere i commenti alle seguenti righe presenti nel file di configurazione:

```
# [general]
# password-db = passwd
```

Dopo aver tolto i commenti alle righe precedenti, è possibile gestire la lista degli utenti nel file passwd. Modificare il file `passwd` presente nella directory e inserire il nuovo utente. La sintassi da usare è la seguente:

```
username = password
```

Per maggiori informazioni fare riferimento al file.

Per accedere a Subversion attraverso il protocollo svn://, sia dalla stessa macchina sia da un'altra macchina, avviare svnserver utilizzando il comando svnserve. La sintassi è la seguente:

```
$ svnserve -d --foreground -r /percorso/al/repository
# -d -- daemon mode
# --foreground -- run in foreground (useful for debugging)
# -r -- root of directory to serve

Per ulteriori dettagli sull'utilizzo fare riferimento a:
$ svnserve --help
```

Una volta eseguito questo comando, Subversion si mette in ascolto sulla porta predefinita (3690). Per accedere al repository del progetto, è necessario eseguire, da un terminale, il seguente comando:

```
svn co svn://hostname/project project --username nome_utente
```

In base alla configurazione del server, verrà richiesta la password. Una volta autenticati, viene eseguito il check out del codice dal repository di Subversion. Per sincronizzare il repository del progetto con la copia locale, è possibile eseguire il comando **update**. La sintassi del comando è la seguente:

```
cd DIRECTORY_DEL_PROGETTO ; svn update
```

Per maggiori informazioni sui sotto comandi di Subversion fare riferimento al manuale. Per esempio, per informazioni sul comando co (checkout), al prompt dei comandi digitare:

```
svn co help
```

2.3.5. Accesso con protocollo personalizzato a cifratura SSL (svn+ssh://)

La configurazione e le procedure sono le medesime del metodo svn:// . Per i dettagli consultare la sezione precedente. Questo passaggio prevede che sia stata seguita la procedura precedente e il server Subversion sia stato avviato con il comando svnserve.

Si suppone che il server ssh sia in esecuzione sulla macchina e che accetti connessioni in entrata. Per una conferma, provare a collegarsi alla macchina attraverso SSH. Se il login viene eseguito, tutto è configurato. In caso contrario configurare SSH.

Il protocollo svn+ssh:// è utilizzato per accedere al repository di Subversion usando la cifratura SSL. I dati che vengono trasmessi sono cifrati con questo metodo. Per accedere al repository del progetto (per esempio attraverso un checkout), utilizzare, con il comando, la sintassi seguente:

```
svn co svn+ssh://hostname/var/svn/repos/project
```

È necessario utilizzare il percorso completo (/percorso/al/repository/progetto) per accedere al repository di Subversion utilizzando questo metodo di accesso.

In base alla configurazione del server, viene richiesta la password. Utilizzare la password per il login con SSH. Una volta autenticati, viene eseguito il checkout del codice dal repository di Subverison.

3. Server CVS

CVS è un sistema di controllo della versione che è possibile utilizzare per registrare i cambiamenti al codice sorgente di un programma.

3.1. Installazione

Per installare CVS, eseguire il seguente comando in un terminale:

```
sudo apt-get install cvs
```

Una volta installato cvs, installare xinetd per avviare/fermare il server CVS. In un terminale, digitare quando segue per installare xinetd:

```
sudo apt-get install xinetd
```

3.2. Configurazione

Once you install cvs, the repository will be automatically initialized. By default, the repository resides under the /srv/cvs directory. You can change this path by running following command:

```
cvs -d /your/new/cvs/repo init
```

Once the initial repository is set up, you can configure xinetd to start the CVS server. You can copy the following lines to the `/etc/xinetd.d/cvspserver` file.

```
service cvspserver
{
     port = 2401
     socket_type = stream
     protocol = tcp
     user = root
     wait = no
     type = UNLISTED
     server = /usr/bin/cvs
     server_args = -f --allow-root /srv/cvs pserver
     disable = no
}
```

Assicurarsi di modificare il repository nel caso in cui sia stata modificata la directory predefinita del repository (/srv/cvs).

Once you have configured xinetd you can start the cvs server by running following command:

```
sudo service xinetd restart
```

Per avere la conferma che il server CVS è in esecuzione, digitare il seguente comando:

```
sudo netstat -tap | grep cvs
```

L'output del comando precedente dovrebbe essere:

```
tcp 0 0 *:cvspserver *:* LISTEN
```

A questo punto è possibile aggiungere altri utenti, nuovi progetti e gestire il server CVS.

CVS consente di aggiungere nuovi utenti indipendentemente dal sistema operativo. Il modo più semplice è utilizzare l'utente Linux per CVS, benché presenti dei problemi di sicurezza. Per maggiori informazioni, consultare il manuale di CVS.

3.3. Aggiungere progetti

Questa sezione spiega come aggiungere nuovi progetti a un repository CVS, creare la directory, aggiungervi i documenti necessari e i file sorgente. Per aggiungere un progetto al repository CVS, eseguire le seguenti istruzioni:

```
cd your/project
cvs -d :pserver:nomeutente@nomehost.com:/srv/cvs import -m \
"Importazione del mio progetto nel repository CVS" . new_project start
```

È possibile utilizzare la variabile d'ambiente CVSROOT per memorizzare la directory root di CVS. Una volta esportata, si può evitare di utilizzare l'opzione «-d» nel comando precedente.

La stringa *new_project* è un tag del fornitore, e *start* è una stringa di rilascio. Non servono a nulla in questo contesto, ma visto che CVS le richiede, vanno inserite.

Quando si aggiunge un nuovo progetto, l'utente CVS deve avere i permessi di scrittura per il repository CVS (/srv/cvs). Per impostazione predefinita, il gruppo src possiede tali permessi: basta quindi semplicemente aggiungere l'utente a questo gruppo per permettergli di gestire progetti nel repository CVS.

4. Riferimenti

Sito web di Bazaar[4]

Launchpad[5]

Sito web di Subversion[6]

Libro su Subversion[7]

Manuale CVS[8]

Pagina della documentazione della comunità su Easy Bazaar[9]

Pagina della documentazione della comunità su Subversion[10]

4 http://bazaar.canonical.com/en/
5 https://launchpad.net/
6 http://subversion.tigris.org/
7 http://svnbook.red-bean.com/
8 http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html
9 https://help.ubuntu.com/community/EasyBazaar
10 https://help.ubuntu.com/community/Subversion

Capitolo 18. Reti Windows

Spesso le reti di computer sono costituite da sistemi eterogenei e, sebbene gestire una rete composta interamente da computer con Ubuntu sarebbe certamente divertente, alcuni ambienti di rete debbono essere costituiti da sistemi Ubuntu e Microsoft® Windows® che operano insieme in armonia. Questa sezione della guida di Ubuntu introduce i principi e gli strumenti utilizzati nella configurazione di un server Ubuntu per la condivisione di risorse di rete con computer Windows.

1. Introduzione

Utilizzare Ubuntu in una rete composta da client Windows significa fornire e integrare i servizi tipici degli ambienti Windows. Questi servizi offrono supporto per la condivisione di dati e informazioni riguardo i computer e gli utenti della rete e possono essere classificati, in base alle loro funzionalità, in tre principali categorie:

- **Servizi per la condivisione di file e stampanti**. Utilizzo del protocollo SMB (Server Message Block) per agevolare la condivisione di file, cartelle, volumi e stampanti attraverso la rete.
- **Servizi di directory**. Condivisione di informazioni vitali sui computer e sugli utenti della rete con l'uso di tecnologie come LDAP (Lightweight Directory Access Protocol) e Microsoft Active Directory®.
- **Autenticazione e accesso**. Stabilire l'identità del computer o dell'utente della rete e determinare quali risorse siano accessibili al computer o all'utente tramite i permessi e i privilegi, utilizzando permessi dei file, politiche di gruppo e il servizio di autenticazione Kerberos.

Fortunatamente, i sistemi Ubuntu sono in grado di fornire queste funzionalità ai client Windows, permettendo la condivisione di risorse di rete. Uno dei componenti software principali, incluso nei sistemi Ubuntu per le operazioni di rete con Windows, è la suite SAMBA, che comprende strumenti e applicazioni per server SMB.

Questa sezione della guida server di Ubuntu è un'introduzione all'uso di Samba e a come installare e configurare i pacchetti necessari. Per maggiori informazioni e documentazione su Samba, consultare il *sito web di Samba*[1].

[1] http://www.samba.org

2. Server di file Samba

Una delle opzioni più comuni per mettere in comunicazione computer con Ubuntu e Windows, è quella di configurare Samba come server di file. Questa sezione spiega come configurare un server Samba per la condivisione di file con client Windows.

Il server viene configurato per condividere file con qualsiasi client nella rete senza dover usare una password. Se all'interno del proprio ambiente di lavoro è richiesto un maggior controllo sugli accessi, consultare *Sezione 4, «Sicurezza di un server di file e di stampa Samba» [284]*

2.1. Installazione

Per prima cosa installare il pacchetto samba. Alla riga di comando, digitare:

```
sudo apt-get install samba
```

Questo è quanto. Ora è possibile configurare Samba affinché possa condividere i file.

2.2. Configurazione

Il file principale di configurazione di Samba è localizzato in `/etc/samba/smb.conf` e dispone di molti commenti utili nella configurazione delle varie direttive.

Non tutte le opzioni disponibili sono incluse nel file di configurazione predefinito. Per maggiori informazioni, consultare la pagina man di `smb.conf` oppure «*Samba HOWTO Collection*[2]».

1. Per prima cosa, modificare le seguenti coppie chiave/valore nella sezione *[global]* del file `/etc/samba/smb.conf`:

   ```
   workgroup = ESEMPIO
   ...
   security = user
   ```

   Il parametro *security* è più avanti nella sezione [global] ed è commentato. Inoltre, modificare *ESEMPIO* in modo che rispecchi il proprio ambiente di lavoro.

2. Per la nuova directory da condividere, creare una nuova sezione verso la fine del file oppure togliere il commento a uno degli esempi:

   ```
   [share]
       comment = Condivisione file Ubuntu
       path = /srv/samba/share
       browsable = yes
       guest ok = yes
       read only = no
   ```

[2] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

```
create mask = 0755
```

- *comment*: una breve descrizione della condivisione. Modificarla in base alle proprie esigenze.
- *path*: il percorso alla directory da condividere.

  Questo esempio utilizza `/srv/samba/sharename` poiché, in base alla *Filesystem Hierarchy Standard (FHS), /srv*[3] è la posizione in cui dovrebbero essere tenuti i file relativi ai siti. Tecnicamente, le condivisione Samba possono essere posizionate ovunque all'interno del file system, basta che i permessi siano impostati correttamente. In ogni caso, è raccomandato aderire agli standard.
- *browsable*: abilita i client Windows a esplorare la directory condivisa usando Windows Explorer.
- *guest ok*: consente ai client di connettersi alla condivisione senza dover fornire una password.
- *sola lettura:* determina se la condivisione è di sola lettura o se sono garantiti anche i privilegi di scrittura. I privilegi di scrittura sono consentiti solo quando il valore è *no*, come mostrato nell'esempio. Se il valore è *si*, allora l'accesso alla condivisione è in sola lettura.
- *create mask*: determina i permessi dei nuovi file creati.

3. Ora che Samba è configurato, è necessario creare la directory e modificarne i permessi. Da un terminale digitare:

```
sudo mkdir -p /srv/samba/share
sudo chown nobody.nogroup /srv/samba/share/
```

L'opzione *-p* indica a mkdir di creare l'intero albero delle directory se questo non esiste.

4. Infine, riavviare il servizio samba per abilitare la nuova configurazione:

```
sudo restart smbd
sudo restart nmbd
```

La configurazione precedente fornisce accesso completo a tutti i client nella rete locale. Per una configurazione più sicura, consultare *Sezione 4, «Sicurezza di un server di file e di stampa Samba» [284]*.

Da un client Windows dovrebbe ora essere possibile esplorare il server di file Ubuntu e visualizzare la directory condivisa. Se il client non mostrasse automaticamente la condivisione, provare ad accedere al server dal suo indirizzo IP, per es. \\192.168.1.1, in una finestra di Windows Explorer. Per verificare che tutto funzioni, provare a creare una directory da Windows.

Per creare ulteriori condivisioni basta creare delle nuove sezioni *[dir]* nel file `/etc/samba/smb.conf` e riavviare *Samba*. Assicurarsi che le directory da condividere esistano e abbiano i permessi impostati correttamente.

[3] http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM

La condivisione chiamata *«[share]»* e il percorso `/srv/samba/share` sono solo esempi. Impostare il nome della condivisione e il percorso per adattarli al contesto: è una buona idea attribuire a una condivisione lo stesso nome di una directory del file system; un altro esempio potrebbe essere una condivisione chiamata *[qa]* con un percorso `/srv/samba/qa`.

2.3. Risorse

- Per delle configurazioni più dettagliate riguardo Samba, consultare *Samba HOWTO Collection*[4]
- La guida è disponibile anche in *formato cartaceo*[5].
- Il libro *Using Samba*[6] di O'Reilly è un'altra buona lettura.
- La pagina *su Samba*[7] della documentazione.

[4] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
[5] http://www.amazon.com/exec/obidos/tg/detail/-/0131882228
[6] http://www.oreilly.com/catalog/9780596007690/
[7] https://help.ubuntu.com/community/Samba

3. Server di stampa Samba

Un' altra configurazione molto comune di Samba è come condivisione di stampanti installate, localmente o in remoto, su un server Ubuntu. Come *Sezione 2, «Server di file Samba» [279]*, questa sezione spiega come configurare Samba affinché qualsiasi client sulla rete locale possa utilizzare le stampanti installate senza la necessità di fornire nome utente o password.

Per una configurazione più sicura, consultare *Sezione 4, «Sicurezza di un server di file e di stampa Samba» [284]*.

3.1. Installazione

Prima di installare e configurare Samba è utile prima di tutto avere un'installazione funzionante di CUPS. Per maggiori informazioni, consultare *Sezione 4, «CUPS - Server di stampa» [232]*.

Per installare il pacchetto samba, da un terminale digitare:

```
sudo apt-get install samba
```

3.2. Configurazione

Dopo l'installazione di Samba, modificare `/etc/samba/smb.conf`: cambiare l'attributo *workgroup* con quello adatto alla propria rete e *security* con *user*:

```
workgroup = ESEMPIO
...
security = user
```

Nella sezione *[printers]* modificare l'opzione *guest ok* a *yes*:

```
browsable = yes
guest ok = yes
```

Una volta modificato il file `smb.conf`, riavviare Samba:

```
sudo restart smbd
sudo restart nmbd
```

La configurazione predefinita di Samba condividerà automaticamente qualsiasi stampante installata. Basta installare la stampante localmente sui client Windows.

3.3. Risorse

- Per delle configurazioni più dettagliate riguardo Samba, consultare *Samba HOWTO Collection*[8]

[8] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

- La guida è disponibile anche in *formato cartaceo*[9].
- Il libro *Using Samba*[10] di O'Reilly è un'altra buona lettura.
- Per maggiori informazioni sulla configurazione di CUPS, consultare il *sito web di CUPS*[11].
- La pagina *su Samba*[12] della documentazione.

[9] http://www.amazon.com/exec/obidos/tg/detail/-/0131882228
[10] http://www.oreilly.com/catalog/9780596007690/
[11] http://www.cups.org/
[12] https://help.ubuntu.com/community/Samba

4. Sicurezza di un server di file e di stampa Samba

4.1. Modalità di sicurezza di Samba

Esistono due livelli di sicurezza disponibili al protocollo CIFS (Common Internet Filesystem): a livello *utente* e a livello *condivisione*. L'implementazione della *modalità di sicurezza* di Samba consente una maggiore flessibilità, fornendo quattro modi per implementare la sicurezza a livello utente e uno per quella a livello condivisione.

- *security = user*: richiede a client di fornire nome utente e password per collegarsi alla condivisione. Gli account di Samba sono separati da quelli di sistema, ma il pacchetto libpam-smbpass consente di sincronizzare utenti e password con il database degli utenti di Samba.
- *security = domain*: questa modalità consente al server Samba di apparire ai client Windows come «Primary Domain Controller» (PDC), «Backup Domain Controller» (BDC) oppure «Domain Member Server» (DMS). Per maggiori informazioni, consultare *Sezione 5, «Samba come controller di dominio» [289]*.
- *security = ADS*: consente al server Samba di unirsi a un dominio «Active Directory» come membro nativo. Per maggiori informazioni, consultare *Sezione 6, «Integrare Samba con Active Directory» [294]*.
- *security = server*: questa modalità non dovrebbe essere usata per motivi di sicurezza. Per maggiori informazioni, consultare la sezione *Server Security*[13] della guida di Samba.
- *security = share*: consente ai client di collegarsi alle condivisioni senza fornire nome utente e password.

La modalità di sicurezza scelta dipende dal proprio ambiente di lavoro e da cosa si vuole ottenere col server Samba.

4.2. Livello di sicurezza utente

Questa sezione spiega come riconfigurare i server di file e di stampa Samba, come spiegato in *Sezione 2, «Server di file Samba» [279]* e *Sezione 3, «Server di stampa Samba» [282]*, affinché richieda l'autenticazione.

Per prima cosa, installare il pacchetto libpam-smbpass che consente di sincronizzare gli utenti di sistema col database degli utenti di Samba:

```
sudo apt-get install libpam-smbpass
```

Se è stato scelto il task *Server Samba* durante l'installazione, il pacchetto libpam-smbpass è già installato.

Aprire il file `/etc/samba/smb.conf` e nella sezione *[share]* modificare:

[13] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id349531

```
guest ok = no
```

Riavviare Samba affinché le nuove impostazioni abbiano effetto:

```
sudo restart smbd
sudo restart nmbd
```

Ora, collegandosi alle directory o alle stampanti condivise, verranno richiesti il nome utente e la password.

Se si sceglie di mappare un drive di rete alla condivisione, selezionare la casella di spunta «Reconnect at Logon» affinché sia possibile inserire nome utente e password solo una volta, almeno finché la password non viene cambiata.

4.3. Livello di sicurezza condivisione

Ci sono diverse opzioni disponibili per aumentare la sicurezza di ogni singola directory condivisa. Facendo uso dell'esempio *[share]*, questa sezione illustra alcune di queste opzioni.

4.3.1. Gruppi

I gruppi definiscono un insieme di computer e utenti che godono dei medesimi privilegi di accesso alle risorse condivise, offrendo un alto livello di controllo di questi accessi. Per esempio, se il gruppo *qa* contiene gli utenti *freda*, *danika* e *rob* e viene definito il secondo gruppo *support* che contiene gli utenti *danika*, *jeremy* e *vincent*, allora alcune risorse di rete impostate per concedere l'accesso al gruppo *qa* concedono automaticamente l'accesso anche agli utenti freda, danika e rob, mentre lo negano a jeremy o vincent. Dal momento che l'utente *danika* è membro di entrambi i gruppi *qa* e *support* potrà accedere a tutte le risorse condivise il cui accesso è stato concesso a entrambi i gruppi, gli altri utenti avranno accesso alle risorse esplicitamente assegnate al gruppo di appartenenza.

Samba, in modo predefinito, controlla i gruppi di sistema locali definiti in `/etc/group` per determinare quali utenti appartengono a quali gruppi. Per maggiori informazioni su come aggiungere o rimuovere gruppi, consultare *Sezione 1.2, «Aggiungere e rimuovere utenti» [155]*.

Quando si definiscono i gruppi nel file di configurazione di Samba, `/etc/samba/smb.conf`, la sintassi predefinita è quella di usare il prefisso «@» col nome del gruppo. Per esempio, per definire il gruppo *sysadmin* in una sezione del file `/etc/samba/smb.conf`, bisogna inserire il nome del gruppo come **@sysadmin**.

4.3.2. Permessi dei file

I permessi dei file definiscono i diritti che un computer o un utente ha su una particolare directory, file o insieme di file. Tali permessi possono essere definiti modificando il file `/etc/samba/smb.conf` e specificando i permessi di una condivisione definita.

Per esempio, se è stata definita una condivisione Samba chiamata *share* e si vuole dare il permesso di *sola lettura* al gruppo di utenti conosciuto come *qa*, ma si vuole concedere permesso di scrittura

sulla condivisione al gruppo *sysadmin* e all'utente *vincent*, modificare il file `/etc/samba/smb.conf` e aggiungere quanto segue al di sotto della sezione *[share]*:

```
read list = @qa
write list = @sysadmin, vincent
```

Un altro possibile permesso con Samba consente di usare i permessi *amministrativi* su una particolare risorsa condivisa. Gli utenti con permessi amministrativi possono leggere, scrivere o modificare qualsiasi informazione all'interno della risorsa per cui sono stati abilitati.

Per esempio, per concedere all'utente *melissa* permessi amministrativi all'interno dell'esempio *share*, modificare il file `/etc/samba/smb.conf` e aggiungere quanto segue al di sotto della sezione *[share]*:

```
admin users = melissa
```

Modificato il file `/etc/samba/smb.conf`, riavviare Samba affinché le modifiche abbiano effetto:

```
sudo restart smbd
sudo restart nmbd
```

Affinché *read list* e *write list* funzionino, il modello di sicurezza di Samba *non* deve essere impostato a *security = share*

Ora che Samba è stato configurato per limitare quali gruppi hanno accesso alla directory condivisa, è necessario aggiornare i permessi del file system.

Il sistema dei permessi sui file di Linux non funziona correttamente con le ACL (Access Control List) di Windows NT. In questi casi, nei server Ubuntu, sono disponibili le ACL POSIX che forniscono un controllo più fine. Per esempio, per abilitare le ACL su `/srv` con file system ext3, modificare il file `/etc/fstab` aggiungendo l'opzione *acl*:

```
UUID=66bcdd2e-8861-4fb0-b7e4-e61c569fe17d /srv  ext3    noatime,relatime,acl 0       1
```

Quindi montare nuovamente la partizione:

```
sudo mount -v -o remount /srv
```

L'esempio precedente assume che `/srv` sia in una partizione separata. Se `/srv` o qualsiasi sia il percorso di condivisione, fa parte della partizione `/`, potrebbe essere necessario riavviare il sistema.

Per uguagliare la configurazione precedente di Samba, al gruppo *sysadmin* devono essere dati i permessi di lettura, scrittura e di esecuzione su `/srv/samba/share`, al gruppo *qa* devono essere dati i permessi di lettura ed esecuzione e i file devono essere di proprietà del nome utente *melissa*. In un terminale, digitare quanto segue:

```
sudo chown -R melissa /srv/samba/share/
sudo chgrp -R sysadmin /srv/samba/share/
sudo setfacl -R -m g:qa:rx /srv/samba/share/
```

Il comando setfacl imposta i permessi di *esecuzione* a tutti i file nella directory `/srv/samba/share`. Nel caso non sia desiderato, non eseguire il comando.

Da un client Windows ora dovrebbe essere possibile notare la nuova implementazione dei permessi dei file. Per maggiori informazioni riguardo le ACL POSIX, consultare le pagine di manuale di acl e setfacl.

4.4. Profilo AppArmor Samba

Ubuntu è dotato del modulo di sicurezza AppArmor, che fornisce un controlli di acceso. Il profilo predefinito di AppArmor per Samba deve essere adattato alla propria configurazione. Per maggiori informazioni sull'uso di AppArmor, consultare *Sezione 4, «AppArmor» [168]*.

All'interno del pacchetto apparmor-profiles sono disponibili dei profili predefiniti di AppArmor per `/usr/sbin/smbd` e `/usr/sbin/nmbd`, i binari dei demoni di Samba. Per installare il pacchetto, da un terminale digitare:

```
sudo apt-get install apparmor-profiles apparmor-utils
```

Questo pacchetto contiene profili per molti altri binari.

I profili per smbd e nmbd sono, in modo predefinito, nella modalità *complain*, consentendo a Samba di lavorare senza dover modificare il profilo e registrando solamente gli errori. Per impostare il profilo smbd in modalità *enforce* e per far funzionare Samba come di consueto, il profilo deve essere modificato per rispecchiare le directory da condividere.

Modificare il file `/etc/apparmor.d/usr.sbin.smbd` aggiungendo informazioni alla sezione *[share]* dall'esempio del server di file:

```
  /srv/samba/share/ r,
  /srv/samba/share/** rwkix,
```

Ora impostare il profilo in modalità *enforce* e ricaricarlo:

```
sudo aa-enforce /usr/sbin/smbd
cat /etc/apparmor.d/usr.sbin.smbd | sudo apparmor_parser -r
```

Dovrebbe essere possibile leggere, scrivere ed eseguire i file nella directory condivisa come di consuetudine e il binario smbd dovrebbe avere accesso solo ai file e le directory configurati. Assicurarsi di aggiungere una voce per ogni directory che viene configurata alla condivisione. Tutti gli errori verranno registrati in `/var/log/syslog`.

4.5. Risorse

- Per delle configurazioni più dettagliate riguardo Samba, consultare *Samba HOWTO Collection*[14]
- La guida è disponibile anche in *formato cartaceo*[15].
- Il libro *Using Samba*[16] di O'Reilly è un'altra buona lettura.
- Il *capitolo 18*[17] della «Samba HOWTO Collection» è dedicato alla sicurezza.
- Il libro *Using Samba*[18] di O'Reilly è un'altra buona lettura.
- La pagina *su Samba*[19] della documentazione.

[14] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
[15] http://www.amazon.com/exec/obidos/tg/detail/-/0131882228
[16] http://www.oreilly.com/catalog/9780596007690/
[17] http://samba.org/samba/docs/man/Samba-HOWTO-Collection/securing-samba.html
[18] http://www.oreilly.com/catalog/9780596007690/
[19] https://help.ubuntu.com/community/Samba

5. Samba come controller di dominio

Benché non possa funzionare come un controller di dominio primario (PDC) Active Directory, un server Samba può essere configurato per apparire come un controller di dominio in stile Windows NT4. Uno dei vantaggi di questa configurazione consiste nell'abilità di centralizzare le credenziali di utenti e computer, inoltre, Samba può utilizzare diversi backend per archiviare le informazioni.

5.1. Controller di dominio primario (PDC)

Questa sezione spiega come configurare Samba come controller di dominio primario (PDC) usando il backend predefinito «smbpasswd».

1. Per prima cosa, installare Samba e libpam-smbpass per sincronizzare gli account utente digitando quanto segue in un terminale:

   ```
   sudo apt-get install samba libpam-smbpass
   ```

2. Configurare Samba modificando il file `/etc/samba/smb.conf`. La variabile *security* dovrebbe essere impostata a *user* e il *workgroup* dovrebbe essere relativo alla propria organizzazione.

   ```
   workgroup = ESEMPIO
   ...
   security = user
   ```

3. Nella sezione commentata «Domains» aggiungere o togliere il commento a quanto segue (l'ultima riga è stata divisa per adattarla al formato di questo documento):

   ```
   domain logons = yes
   logon path = \\%N\%U\profile
   logon drive = H:
   logon home = \\%N\%U
   logon script = logon.cmd
   add machine script = sudo /usr/sbin/useradd -N -g machines -c Machine -d
         /var/lib/samba -s /bin/false %u
   ```


   Per non usare i profili *roaming*, non togliere il commento alle opzioni *logon home* e *logon path*.

   - *domain logons*: fornisce il servizio netlogon facendo in modo che Samba si comporti come un controller di dominio.
   - *logon path*: posiziona il profilo degli utenti Windows all'interno della loro directory home. È possibile anche configurare una condivisione *[profiles]* posizionando tutti i profili all'interno di una sola directory.
   - *logon drive*: specifica il percorso locale della directory home.
   - *logon home*: specifica la posizione della directory home.

- *logon script*: determina quale script eseguire localmente una volta che un utente ha eseguito l'accesso. Lo script deve essere all'interno della condivisione *[netlogon]*.
- *add machine script*: uno script che crea automaticamente lo *Machine Trust Account* necessario per accedere al dominio.

  In questo esempio il gruppo *machines* deve essere creato usando l'utilità addgroup. Per maggiori informazioni, consultare *Sezione 1.2, «Aggiungere e rimuovere utenti» [155]*.

4. Togliere il commento alla condivisione *[homes]* per consentire la mappatura di *logon home*:

```
[homes]
   comment = Home Directories
   browseable = no
   read only = no
   create mask = 0700
   directory mask = 0700
   valid users = %S
```

5. Quando configurato come controller di dominio, è necessario configurare una condivisione *[netlogon]*. Per abilitarla, togliere il commento a:

```
[netlogon]
   comment = Network Logon Service
   path = /srv/samba/netlogon
   guest ok = yes
   read only = yes
   share modes = no
```

Il percorso della condivisione predefinita di *netlogon* è `/home/samba/netlogon`, ma in base allo «Filesystem Hierarchy Standard» (FHS), */srv*[20] è la corretta posizione i cui dovrebbero essere tenuti i file specifici dei siti forniti dal sistema.

6. Creare la directory `netlogon` e un file `logon.cmd` per ora vuoto:

```
sudo mkdir -p /srv/samba/netlogon
sudo touch /srv/samba/netlogon/logon.cmd
```

   È possibile inserire qualsiasi comando di logon Windows in `logon.cmd` per personalizzare l'ambiente del client.

7. Riavviare Samba per abilitare il nuovo controller di dominio:

```
sudo restart smbd
sudo restart nmbd
```

8. Infine, sono richiesti alcuni comandi addizionali per impostare correttamente i permessi.

[20] http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM

Con l'utente *root* disabilitato in modo predefinito, per poter inserire una workstation nel dominio, un gruppo di sistema deve essere mappato al gruppo Windows *Domain Admins*. Usando l'utilità net, da un terminale digitare:

```
sudo net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin rid=512 type=d
```

Modificare *sysadmin* con un qualsiasi altro gruppo si voglia usare. Inoltre, l'utente usato per unirsi al dominio deve essere membro del gruppo *sysadmin* oltre al gruppo *admin*. Il gruppo *admin* consente l'utilizzo di sudo.

Se l'utente non dispone ancora di credenziali Samba, è possibile crearle con l'utilità smbpasswd, modificando opportunamente il nome utente *sysadmin*:

```
sudo smbpasswd -a sysadmin
```

Inoltre, è necessario fornire i diritti al gruppo *Domain Admins* per consentire ad *add machine script* (e altre funzioni di amministrazione) di funzionare. Per fare ciò:

```
net rpc rights grant -U sysadmin "EXAMPLE\Domain Admins" SeMachineAccountPrivilege \ SePrintOpe
```

9. Dovrebbe ora essere possibile unire i client Windows al dominio come in un dominio NT4 in esecuzione su un server Windows.

5.2. Controller di dominio di backup

Con la presenza di un controller di dominio primario (PDC) all'interno delle rete è utile avere anche un controller di dominio di backup (BDC). In questo modo i client potranno autenticarsi anche nel caso in cui il PDC non sia più disponibile.

Quando si configura Samba come BDC, è necessario avere un metodo di sincronizzazione delle informazioni sugli account con il PDC. A questo scopo è possibile usare scp, rsync oppure LDAP come backend *passdb*.

Il metodo migliore per sincronizzare le informazioni sugli account consiste nell'usare LDAP, poiché entrambi i controller di dominio possono usare le stesse informazioni in tempo reale. Configurare un server LDAP potrebbe essere troppo complicato per un esiguo numero di utenti e computer. Per maggiori informazioni, consultare *Sezione 2, «Samba e LDAP» [119]*.

1. Installare samba e libpam-smbpass. Da un terminale digitare:

```
sudo apt-get install samba libpam-smbpass
```

2. Modificare il file `/etc/samba/smb.conf` e togliere il commento a quanto segue nella sezione *[global]*:

```
workgroup = ESEMPIO
...
security = user
```

3. Nella sezione *Domains* togliere il commento o aggiungere quanto segue:

```
domain logons = yes
domain master = no
```

4. Assicurarsi che un utente abbia i permessi di lettura sui file in `/var/lib/samba`. Per esempio, per consentire agli utenti del gruppo *admin* di eseguire scp sui file, digitare:

```
sudo chgrp -R admin /var/lib/samba
```

5. Sincronizzare gli account utente usando scp per copiare la directory `/var/lib/samba` dal PDC:

```
sudo scp -r NOME_UTENTE@PDC:/var/lib/samba /var/lib
```

Sostituire *NOME_UTENTE* con un nome utente valido e *PDC* con il nome host o l'indirizzo IP del controller di dominio primario.

6. Riavviare samba:

```
sudo restart smbd
sudo restart nmbd
```

È possibile verificare se il controller di dominio di backup è funzionante fermando il demone Samba sul PDC e quindi cercando di eseguire l'accesso su un client Windows all'interno del dominio.

È utile ricordare anche che se è stata configurata l'opzione *logon home* come directory sul PDC e quest'ultimo non è più disponibile, anche l'accesso al drive *home* degli utenti non lo sarà. Per questo motivo è utile configurare *logon home* affinché sia posizionato in un server di file separato da PDC e BDC.

5.3. Risorse

- Per delle configurazioni più dettagliate riguardo Samba, consultare *Samba HOWTO Collection*[21]
- La guida è disponibile anche in *formato cartaceo*[22].
- Il libro *Using Samba*[23] di O'Reilly è un'altra buona lettura.
- Il *capitolo 4*[24] della «Samba HOWTO Collection» spiega come configurare un controller di dominio primario.
- Il *capitolo 5*[25] della «Samba HOWTO Collection» spiega come configurare un controller di dominio di backup.

21 http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
22 http://www.amazon.com/exec/obidos/tg/detail/-/0131882228
23 http://www.oreilly.com/catalog/9780596007690/
24 http://samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-pdc.html
25 http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html

- La pagina *su Samba*[26] della documentazione.

[26] https://help.ubuntu.com/community/Samba

6. Integrare Samba con Active Directory

6.1. Accedere a una condivisione Samba

Un altro uso di Samba consiste nell'integrarlo all'interno di una rete Windows esistente. Una volta parte di un dominio Active Directory, Samba può fornire servizi di file e stampa agli utenti AD.

The simplest way to join an AD domain is to use Likewise-open. For detailed instructions see the *Likewise Open documentation*[27].

Una volta entrati nel dominio Active Directory, digitare il seguente comando in un terminale:

```
sudo apt-get install samba smbfs smbclient
```

Aprire il file `/etc/samba/smb.conf` e modificare quanto segue:

```
workgroup = EXAMPLE
...
security = ads
realm = EXAMPLE.COM
...
idmap backend = lwopen
idmap uid = 50-9999999999
idmap gid = 50-9999999999
```

Riavviare samba affinché le nuove impostazioni abbiano effetto:

```
sudo restart smbd
sudo restart nmbd
```

Dovrebbe essere ora possibile accedere qualsiasi condivisione Samba da un client Windows. Assicurarsi comunque di concedere agli utenti o ai gruppi AD accesso alla directory condivisa. Per maggiori informazioni, consultare *Sezione 4, «Sicurezza di un server di file e di stampa Samba» [284]*.

6.2. Accedere a una condivisione Windows

Ora che il server Samba è parte del dominio Active Directory, è possibile accedere a qualsiasi condivisione server di Windows:

- Per montare una condivisione file di Windows, in un terminale digitare quanto segue:

  ```
  mount.cifs //fs01.example.com/share mount_point
  ```

  È possibile accedere alle condivisioni su computer non facenti parte del dominio AD, ma sarà necessario fornire un nome utente e una password.

[27] http://www.beyondtrust.com/Technical-Support/Downloads/files/pbiso/Manuals/ubuntu-active-directory.html

- Per montare la condivisione durante la fase di avvio, aggiungere una voce al file `/etc/fstab`, per esempio:

```
//192.168.0.5/share /mnt/windows cifs auto,username=steve,password=secret,rw 0        0
```

- Un altro modo per copiare i file da un server Windows consiste nell'usare l'utilità smbclient. Per elencare i file presenti in una condivisione Windows:

```
smbclient //fs01.example.com/share -k -c "ls"
```

- Per copiare un file da una condivisione, digitare:

```
smbclient //fs01.example.com/share -k -c "get file.txt"
```

  In questo modo si copierà il file `file.txt` nella directory corrente.

- Per copiare una file nella condivisione:

```
smbclient //fs01.example.com/share -k -c "put /etc/hosts hosts"
```

  In questo modo il file `/etc/hosts` verrà copiato in `//fs01.example.com/share/hosts`.

- L'opzione *-c* usata nei comandi precedenti consente di eseguire il comando smbclient in una sola volta. Questo è utile all'interno di script e per altre operazioni sui file. Per accedere al prompt *smb: \>*, un prompt simile a quello di FTP dove è possibile svolgere normali operazioni su file e directory, digitare:

```
smbclient //fs01.example.com/share -k
```

Sostituire tutte le occorrenze di *fs01.example.com/share*, *//192.168.0.5/share*, *username=steve,password=secret* e *file.txt* con l'indirizzo IP del proprio server, il nome nome host, il nome della condivisione, il nome del file e il nome utente e la password dell'utente a cui è consentito accedere alla condivisione.

6.3. Risorse

For more smbclient options see the man page: **man smbclient**, also available *online*[28].

The mount.cifs *man page*[29] is also useful for more detailed information.

La pagina *su Samba*[30] della documentazione.

[28] http://manpages.ubuntu.com/manpages/quantal/en/man1/smbclient.1.html
[29] http://manpages.ubuntu.com/manpages/quantal/en/man8/mount.cifs.8.html
[30] https://help.ubuntu.com/community/Samba

Capitolo 19. Backup

È possibile eseguire dei backup delle installazioni di Ubuntu in molti modi diversi. La fase più importante è comunque quella della *pianificazione*: di cosa eseguire il backup, dove salvarlo e come ripristinarlo.

Questa sezione descrive diversi metodi per compiere queste attività.

1. Script shell

Uno dei metodi più semplici per effettuare il backup del sistema è usare uno*shell script*. Per esempio, è possibile usare uno script per scegliere le directory da archiviare e usare queste directory come argomento per l'utilità tar per creare un archivio, che può essere quindi spostato o copiato in un'altra posizione. L'archivio può anche essere creato su un file system remoto, come una condivisione *NFS* .

L'utilità tar crea un archivio di file a partire da molti file o directory. Con tar è possibile anche elaborare i file con utilità di compressione riducendo così la dimensione dell'archivio.

1.1. Semplice script shell

Il seguente script utilizza tar per creare un archivio su un file system remoto NFS. Il nome dell'archivio è determinato utilizzando delle utilità a riga di comando aggiuntive.

```
#!/bin/sh
####################################
#
# Backup to NFS mount script.
#
####################################

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/mnt/backup"

# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest
```

- *$backup_files*: una variabile con le directory di cui si vuole fare una copia. L'elenco va modificato come desiderato.
- *$day:*: una variabile contenente il giorno della settimana (lunedì, martedì, mercoledì, ecc...) viene usata per creare un archivio per ogni giorno della settimana, consentendo di avere una cronologia di archivi di sette giorni. Esistono altri metodi per fare questo, come l'uso dell'utilità date.
- *$hostname*: variabile contenente il nome host *breve* del sistema. Usare il nome dell'host nel nome dell'archivio, consente di avere backup giornalieri di diversi sistemi in una sola directory.
- *$archive_file*: il nome completo dell'archivio.
- *$dest:* destinazione dell'archivio. La directory deve essere creata e in questo caso anche *mounted* prima di eseguire lo script di backup. Per dettagli sull'uso di *NFS*, consultare la relativa sezione *Sezione 2, «NFS (Network File System)» [227]*.
- *messaggi:* messaggi opzionali stampati sulla console usando echo.
- *tar czf $dest/$archive_file $backup_files*: il comando tar usato per creare l'archivio.
  - *c*: crea l'archivio.
  - *z*: passa l'archivio attraverso l'utilità di compressione gzip.
  - *f:* usa un file archivio, altrimenti il comando tar invia l'output sullo STDOUT.
- *ls -lh $dest*: istruzione opzionale che stampa un elenco lungo (-*l*) in un formato leggibile (-*h*) della directory di destinazione. È utile per controllare la dimensione dell'archivo. Questa verifica non dovrebbe sostituire la verifica dell'archivio.

Questo è un semplice esempio di un backup eseguito con uno script shell ed è possibile aggiungere molte opzioni. Per maggiori informazioni sugli script shell, consultare la sezione *Sezione 1.4, «Riferimenti» [300]*.

1.2. Eseguire lo script

1.2.1. Esecuzione da terminale

Il metodo più facile per eseguire lo script di backup è quello di copiare il contenuto dello script in un file, `backup.sh` per esempio, ed eseguirlo in un terminale:

```
sudo bash backup.sh
```

È un ottimo modo per provare lo script e assicurarsi che funzioni correttamente.

1.2.2. Esecuzione con cron

L'utilità cron può essere usata per automatizzare l'esecuzione dello script. Il demone cron consente l'esecuzione di script o comandi a un determinato orario e data.

L'applicazione cron è configurata attraverso delle voci in un file `crontab` file. I file `crontab` sono separati in campi:

```
# m h dom mon dow   comando
```

- *m:* minuto di esecuzione del comando, tra 0 e 59.
- *h:* ora di esecuzione del comando, tra 0 e 23.
- *dom*: giorno del mese di esecuzione del comando.
- *mon:* mese in cui viene eseguito il comando, tra 1 e 12.
- *dow:* giorno della settimana in cui viene eseguito il comando, tra 0 e 7. La domenica può essere specificata usando sia 0 che 7.
- *comando*: il comando da eseguire.

Per aggiungere o modificare voci in un file `crontab`, dovrebbe essere usato il comando crontab -e, i contenuti di un file `crontab` possono essere visualizzati usando il comando crontab -l.

Per eseguire lo script backup.sh usando cron, in un terminale digitare quanto segue:

```
sudo crontab -e
```

Usare sudo con il comando crontab -e, modifica il crontab dell'utente *root*. Questo è necessario nel caso in cui si stiano eseguendo copie di backup di file accessibili solo dall'utente root.

Aggiungere quanto segue al file `crontab`:

```
# m h dom mon dow   command
0 0 * * * bash /usr/local/bin/backup.sh
```

Lo script backup.sh verrà eseguito ogni giorno alle 12.00 AM.

Lo script backup.sh deve essere copiato nella directory `/usr/local/bin/` perché questa voce venga eseguita correttamente. Lo script può risiedere ovunque nel file system, basta cambiare il percorso in modo appropriato.

Per maggiori dettagli sulle opzioni di crontab, conultare *Sezione 1.4, «Riferimenti» [300]*.

1.3. Ripristinare l'archivio

Una volta creato un archivio, è importante verificarlo, elencandone i contenuti oppure, ed è la scelta migliore, *ripristinare* un file dall'archivio.

- Per visualizzare un elenco dei contenuti di un archivio, digitare in una riga di comando di un terminale:

  ```
  tar -tzvf /mnt/backup/host-lunedì.tgz
  ```

- Per ripristinare un file dall'archivio in una directory diversa, digitare:

```
tar -xzvf /mnt/backup/host-lunedì.tgz -C /tmp etc/hosts
```

L'opzione *-C* di tar redirige i file estratti nella directory specificata. L'esempio precedente estrarrà il file `/etc/hosts` in `/tmp/etc/hosts`. La struttura della directory viene quindi ricreata da tar.

Notare anche che il simbolo «/» iniziale del percorso in cui ripristinare è stato tralasciato.

- Per ripristinare tutti i file presenti nell'archivio, digitare:

```
cd /
sudo tar -xzvf /mnt/backup/host-lunedì.tgz
```

In questo modo verranno sovrascritti i file attualmente presenti nel file system.

1.4. Riferimenti

- Per maggiori informazioni riguardo lo script da shell, consultare la *Advanced Bash-Scripting Guide*[1]
- Il libro *Teach Yourself Shell Programming in 24 Hours*[2] è disponibile in linea ed è un'ottima risorsa per lo script da shell.
- La pagina della *della documentazione in linea su cron*[3] contiene ulteriori dettagli sulle opzioni avanzate di cron.
- Per maggiori informazioni sulle opzioni del comando tar, consultare il *manuale in linea di tar*[4].
- La pagina inglese di Wikipedia *Backup Rotation Scheme*[5] contiene informazioni sugli schemi di backup.
- Questo script utilizza tar per creare l'archivio, ma esistono diverse altre utilità a riga di comando che possono essere usate, per esempio:
  - *cpio*[6]: usata per copiare file da e verso degli archivi.
  - *dd*[7]: parte del pacchetto coreutils. Un'utilità di basso livello per copiare dati da un formato all'altro.
  - *rsnapshot*[8]: una utility per istantanee del file system utilizzata per creare copie di un intero file system.
  - *rsync*[9]: una flessibile utility usata per creare copie incrementali di file.

[1] http://tldp.org/LDP/abs/html/
[2] http://safari.samspublishing.com/0672323583
[3] http://wiki.ubuntu-it.org/AmministrazioneSistema/Cron
[4] http://www.gnu.org/software/tar/manual/index.html
[5] http://en.wikipedia.org/wiki/Backup_rotation_scheme
[6] http://www.gnu.org/software/cpio/
[7] http://www.gnu.org/software/coreutils/
[8] http://www.rsnapshot.org/
[9] http://www.samba.org/ftp/rsync/rsync.html

2. Rotazione degli archivi

Lo script in *Sezione 1, «Script shell» [297]* consente solamente sette archivi differenti. Per un server i cui dati non cambiano molto spesso, questo può essere sufficiente, ma se il server dispone di grossi quantitativi di dati, è necessario avere un più complesso schema di rotazione.

2.1. Rotazione degli archivi NFS

In questa sezione, lo script verrà leggermente modificato per implementare uno schema di rotazione del tipo progenitore-genitore-figlio (mensile-settimanale-giornaliero):

- La rotazione eseguirà un backup *giornaliero* dalla domenica al venerdì.
- Il sabato, viene eseguito un backup *settimanale* consentendo di avere così quattro backup settimanali al mese.
- Il backup *mensile* è eseguito il primo giorno del mese, ruotando due backup mensili se il mese è pari o dispari.

Questo è il nuovo script:

```
#!/bin/bash
####################################
#
# Backup to NFS mount script with
# grandfather-father-son rotation.
#
####################################

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/mnt/backup"

# Setup variables for the archive filename.
day=$(date +%A)
hostname=$(hostname -s)

# Find which week of the month 1-4 it is.
day_num=$(date +%d)
if (( $day_num <= 7 )); then
        week_file="$hostname-week1.tgz"
elif (( $day_num > 7 && $day_num <= 14 )); then
        week_file="$hostname-week2.tgz"
elif (( $day_num > 14 && $day_num <= 21 )); then
        week_file="$hostname-week3.tgz"
elif (( $day_num > 21 && $day_num < 32 )); then
        week_file="$hostname-week4.tgz"
fi
```

```
# Find if the Month is odd or even.
month_num=$(date +%m)
month=$(expr $month_num % 2)
if [ $month -eq 0 ]; then
        month_file="$hostname-month2.tgz"
else
        month_file="$hostname-month1.tgz"
fi

# Create archive filename.
if [ $day_num == 1 ]; then
 archive_file=$month_file
elif [ $day != "Saturday" ]; then
        archive_file="$hostname-$day.tgz"
else
 archive_file=$week_file
fi

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest/
```

Lo script può essere eseguito attraverso gli stessi metodi descritti in *Sezione 1.2, «Eseguire lo script» [298]*.

È utile, nel caso si verifichino disastri, che il dispositivo di backup sia in una località diversa. Nello script di esempio l'unità di backup è un server che fornisce una condivisione NFS: spostare questo server in un'altra località potrebbe non essere fattibile. In base alla velocità di connessione, potrebbe essere utile considerare di copiare il file d'archivio attraverso un collegamento WAN su un server remoto.

Un'altra opzione consiste nel copiare l'archivio su di un disco esterno che può essere spostato. Poiché il prezzo dei dischi portatili esterni è sempre in diminuzione, l'utilizzo di due dischi per ogni livello dell'archivio può risultare altamente vantaggioso: in questo modo è possibile avere un disco esterno collegato al server di backup e un altro in un'altra località.

2.2. Dispositivi a nastro

Invece di usare una condivisione NFS, è possibile utilizzare un dispositivo a nastro collegato al server. Un dispositivo di questo tipo semplifica la rotazione degli archivi e lo spostamento dello stesso dispositivo in un'altra locazione.

Quando viene usato un dispositivo a nastro, la parte dello script relativa al nome del file non è necessaria, in quanto il dato è inviato direttamente al dispositivo, ma sono necessari alcuni comandi per manipolare il nastro. Ciò viene effettuato usando mt, un'utilità di controllo di nastri magnetici parte del pacchetto cpio.

Questo è lo script modificato per l'uso di un dispositivo a nastro:

```
#!/bin/bash
####################################
#
# Backup to tape drive script.
#
####################################

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/dev/st0"

# Print start status message.
echo "Backing up $backup_files to $dest"
date
echo

# Make sure the tape is rewound.
mt -f $dest rewind

# Backup the files using tar.
tar czf $dest $backup_files

# Rewind and eject the tape.
mt -f $dest rewoffl

# Print end status message.
echo
echo "Backup finished"
date
```

Il nome del device predefinito per un dispositivo a nastro SCSI è `/dev/st0`, utilizzare il percorso al device appropriato per il proprio sistema.

Ripristinare i dati da un dispositivo a nastro funziona allo stesso modo di ripristinare da un file. Riavvolgere il nastro e usare il percorso del dispositivo al posto del percorso al file. Per esempio, per ripristinare il file `/etc/hosts` in `/tmp/etc/hosts`:

```
mt -f /dev/st0 rewind
tar -xzf /dev/st0 -C /tmp etc/hosts
```

3. Bacula

Bacula è un programma per eseguire backup, ripristinare e verificare i dati attraverso la rete. Esistono client Bacula per Linux, Windows e Mac OS X, e questo lo rende una soluzione multi-piattaforma.

3.1. Panoramica

Bacula è composto da diversi componenti e servizi usati per gestire i file sui quali eseguire il backup e la posizione del backup stesso:

- Bacula Director: un servizio che controlla tutte le operazioni di backup, ripristino, verifica e di archiviazione.
- Bacula Console: un'applicazione che consente di comunicare con «Director». Sono disponibili tre versioni:
  - Versione testuale per la riga di comando.
  - Versione grafica per GNOME basata su GTK+.
  - Interfaccia wxWidgets.
- Bacula File: conosciuta anche come Bacula Client. Questa applicazione è installata nei computer di cui deve essere fatto il backup ed è responsabile dei dati richiesti dal Director.
- Bacula Storage: il programma che esegue l'archiviazione e il ripristino sul dispositivo fisico.
- Bacula Catalog: responsabile per mantenere l'indice dei file e il database di tutti i file, consentendo una facile localizzazione e ripristino. «Catalog» supporta tre diversi database: MySQL, PostgreSQL e SQLite.
- Bacula Monitor: consente di monitorare i demoni «Director», «File» e «Storage». Attualmente «Monitor» è disponibile solo come applicazione GTK+.

Questi servizi e applicazioni possono essere eseguiti su molteplici server e client oppure possono essere installati su un solo computer se deve essere eseguito il backup di un singolo disco o volume.

3.2. Installazione

Usando MySQL o PostgreSPQ come database, si dovrebbero avere già a disposizione i relativi servizi, in quanto questi non verranno installati da Bacula.

Ci sono molteplici pacchetti che contengono i diversi componenti di Bacula. Per installare Bacula, in un terminale, digitare:

```
sudo apt-get install bacula
```

In modo predefinito, installando il pacchetto bacula viene usato un database MySQL per «Catalog». Se si vuole usare SQLite oppure PostgreSQL, installare bacula-director-sqlite3 o bacula-director-pgsql rispettivamente.

Durante il processo di installazione viene chiesto di fornire delle credenziali per l'*amministratore* del database e per il *proprietario* del database *bacula*. L'amministratore del database deve avere i diritti apporpriati per poter creare un database. Per maggiori informazioni, consultare la *Sezione 1, «MySQL» [207]*.

3.3. Configurazione

I file di configurazione di Bacula sono formattati in base alle *risorse* composte da *direttive* marcate da parantesi «{}». Ogni compoenente di Bacula dispone di un file nella directory `/etc/bacula`.

I diversi componenti di Bacula devono autorizzarsi tra di loro. Questo è fatto usando la direttiva *password*. Per esempio, la risorsa password di *Storage* nel file `/etc/bacula/bacula-dir.conf` deve corrispondere alla risorsa password di *Director* nel file `/etc/bacula/bacula-sd.conf`.

In modo predefinito, il lavoro di backup chiamato *Client1* è configurato per archiviare il «Catalog» di Bacula. Se si intende usare il server per eseguire il backup di più di un client, è necessario modificare il nome del lavoro con qualche cosa di più descrittivo. Per fare questo, modificare il file `/etc/bacula/bacula-dir.conf`:

```
#
# Define the main nightly save backup job
#   By default, this job will back up to disk in
Job {
  Name = "BackupServer"
  JobDefs = "DefaultJob"
  Write Bootstrap = "/var/lib/bacula/Client1.bsr"
}
```

L'esempio precedente modifica il nome del lavoro in *BackupServer*, in corrispondenza del nome host del computer. Sostituire «BackupServer» con il nome host appropriato o un altro nome descrittivo.

Console può essere usato per interrogare *Director* riguardo i lavori, ma per poter usare «Console» con un utente *non-root*, l'utente deve essere nel gruppo *bacula*. Per aggiungere un utente al gruppo «bacula», in un terminale, digitare:

```
sudo adduser NOME_UTENTE bacula
```

Sostituire *NOME_UTENTE* con il vero nome utente. Inoltre, se si sta aggiungendo l'utente corrente al gruppo, è necessario terminare la sessione e rientrarvi affinché le modifiche abbiano effetto.

3.4. Backup locale

Questa sezione descrive come eseguire un backup di specifiche directory di un singolo host in un dispositivo a nastro locale.

- Per prima cosa, *Storage* deve essere configurato. Modificare `/etc/bacula/bacula-sd.conf`:

```
Device {
  Name = "Tape Drive"
  Device Type = tape
  Media Type = DDS-4
  Archive Device = /dev/st0
  Hardware end of medium = No;
  AutomaticMount = yes;               # when device opened, read it
  AlwaysOpen = Yes;
  RemovableMedia = yes;
  RandomAccess = no;
  Alert Command = "sh -c 'tapeinfo -f %c | grep TapeAlert'"
}
```

  L'esempio è relativo a un dispositivo a nastro *DDS-4*. Modificare «Media Type» e «Archive Device» affinché corrispondano al proprio hardware.

  È possibile anche de-commentare uno degli altri file di esempio.

- Una volta modificato il file `/etc/bacula/bacula-sd.conf`, il demone Storage deve essere riavviato:

```
sudo service bacula-sd restart
```

- Ora aggiungere una risorsa *Storage* in `/etc/bacula/bacula-dir.conf` per usare il nuovo «Device»:

```
# Definition of "Tape Drive" storage device
Storage {
  Name = TapeDrive
  # Do not use "localhost" here
  Address = backupserver # N.B. Use a fully qualified name here
  SDPort = 9103
  Password = "Cv70F6pf1t6pBopT4vQOnigDrR0v3LT3Cgkiyjc"
  Device = "Tape Drive"
  Media Type = tape
}
```

  La direttiva *Address* deve essere il «Fully Qualified Domain Name» (FQDN) del server. Modificare quindi *backupserver* col nome host attuale.

  Inoltre, assicurarsi che la direttiva *Password* corrisponda alla stringa in `/etc/bacula/bacula-sd.conf`.

- Creare un nuovo *FileSet*, per determinare di quali directory eseguire il backup:

```
# LocalhostBacup FileSet.
FileSet {
  Name = "LocalhostFiles"
```

```
  Include {
    Options {
      signature = MD5
      compression=GZIP
    }
    File = /etc
    File = /home
  }
}
```

Questo *FileSet* eseguirà il backup delle directory `/etc` e `/home`. La direttiva *Options* configura FileSet per creare una firma MD5 per ciascun file di cui si è eseguito il backup e per comprimere i file con GZIP.

- Creare una nuova sezione *Schedule* per il lavoro di backup:

```
# LocalhostBackup Schedule -- Daily.
Schedule {
  Name = "LocalhostDaily"
  Run = Full daily at 00:01
}
```

Il lavoro verrà eseguito ogni giorno alle 00.01. Sono comunque disponibili molte altre opzioni di pianificazione.

- Infine creare il *Job*:

```
# Localhost backup.
Job {
  Name = "LocalhostBackup"
  JobDefs = "DefaultJob"
  Enabled = yes
  Level = Full
  FileSet = "LocalhostFiles"
  Schedule = "LocalhostDaily"
  Storage = TapeDrive
  Write Bootstrap = "/var/lib/bacula/LocalhostBackup.bsr"
}
```

Questo lavoro creerà un backup *Full* (completo) ogni giorno sul dispositivo a nastro.

- Ogni nastro usato deve avere una *Label*. Se il nastro corrente ne è sprovvisto, Bacula invierà un'email. Per aggiungere un'etichetta a un nastro usando Console, in un terminale, digitare:

```
bconsole
```

- Al prompt di «Console» digitare:

```
label
```

- Viene quindi chiesta la risorsa *Storage*:

```
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
The defined Storage resources are:
     1: File
     2: TapeDrive
Select Storage resource (1-2):2
```

- Inserire il nome del nuovo *Volume* (volume):

```
Enter new Volume name: Sunday
Defined Pools:
     1: Default
     2: Scratch
```

  Sostituire *Sunday* con l'etichetta desiderata.

- Ora selezionare *Pool*:

```
Select the Pool (1-2): 1
Connecting to Storage daemon TapeDrive at backupserver:9103 ...
Sending label command for Volume "Sunday" Slot 0 ...
```

Bacula è ora configurato per eseguire backup del host locale su un dispositivo a nastro.

3.5. Risorse

- Per maggiori informazioni sulle opzioni di configurazione di *Bacula*, consultare il *manuale di Bacula*[10]
- Il sito *di Bacula*[11] contiene le ultime notizie dello sviluppo di Bacula.
- Consultare anche la *documentazione di bacula online*[12].

[10] http://www.bacula.org/en/rel-manual/index.html
[11] http://www.bacula.org/
[12] https://help.ubuntu.com/community/Bacula

Capitolo 20. Virtualizzazione

La virtualizzazione, al giorno d'oggi, viene utilizzata in diversi ambienti e situazioni. Dal punto di vista dello sviluppatore, la virtualizzazione offre un ambiente sicuro dove poter eseguire qualsiasi tipo di sviluppo, senza compromettere l'ambiente di lavoro. Per l'amministratore di sistema, è possibile usare la virtualizzazione per separare facilmente i propri servizi e spostarli in base alle richieste.

The default virtualization technology supported in Ubuntu is KVM. KVM requires virtualization extensions built into Intel and AMD hardware. Xen is also supported on Ubuntu. Xen can take advantage of virtualization extensions, when available, but can also be used on hardware without virtualization extensions. Qemu is another popular solution for hardware without virtualization extensions.

1. libvirt

La libreria libvirt è utilizzata per interfacciarsi con differenti tecnologie di virtualizzazione. Prima di iniziare a utilizzare libvirt è utile accertarsi che il proprio hardware supporti le estensioni di virtualizzazione necessarie per KVM. In un terminale, digitare quanto segue:

```
kvm-ok
```

Verrà stampato un messaggio che indica se la CPU *supporta* o *non supporta* la virtualizzazione hardware.

Nella maggior parte dei processori che supportano la virtualizzazione è necessario attivarla attraverso un'opzione nel BIOS.

1.1. Rete virtuale

Esistono diversi modi per consentire accesso alla rete esterna a una macchina virtuale. La configurazione di rete predefinita è *usermode*, che utilizza il protocollo SLIRP e il traffico è passato attraverso l'interfaccia dell'host verso la rete esterna.

Affinché gli host esterni possano accedere i servizi su una macchina virtuale, è necessario configurare un *bridge*. Questo consente alle interfacce virtuali di connettersi alla rete esterna attraverso l'interfaccia fisica, facendole apparire come normali host al resto della rete. Per informazioni su come impostare un bridge, consultare *Sezione 1.4, «Bridging» [42]*.

1.2. Installazione

Per installare i pacchetti necessari, da un terminale digitare:

```
sudo apt-get install kvm libvirt-bin
```

Dopo aver installato libvirt-bin, l'utente usato per la gestione delle macchine virtuali deve essere aggiunto al gruppo *libvirtd*. In questo modo, all'utente è garantito accesso alle configurazioni avanzate di rete.

In un terminale digitare:

```
sudo adduser $USER libvirtd
```

Se l'utente scelto è quello corrente, è necessario terminare la sessione e ri-accedervi affinché le modifiche abbiano effetto.

È ora possibile installare un sistema operativo *ospite*. La procedura di installazione di una macchina virtuale è la stessa di un sistema operativo normale ed è quindi necessario automatizzare la procedura oppure avere una tastiera e uno schermo collegati al computer.

Nel caso delle macchine virtuali, un'interfaccia grafica è analoga all'uso di una tastiera e di un mouse. Invece di installare un'interfaccia grafica, è possibile usare virt-viewer per connettersi alla console di una macchina virtuale via VNC. Per maggiori informazioni, consultare la *Sezione 1.6, «Visualizzatore di macchine virtuali» [314]*.

There are several ways to automate the Ubuntu installation process, for example using preseeds, kickstart, etc. Refer to the *Ubuntu Installation Guide*[1] for details.

Un altro metodo per installare una macchina virtuale Ubuntu consiste nell'usare l'applicazione ubuntu-vm-builder. ubuntu-vm-builder consente di impostare partizioni avanzate, eseguire script personalizzati post-installazione, ecc... Per maggiori informazioni, consultare *Sezione 2, «JeOS e vmbuilder» [316]*

Libvirt can also be configured work with Xen. For details, see the Xen Ubuntu community page referenced below.

1.3. virt-install

virt-install fa parte del pacchetto virtinst: per installarlo, in un terminale digitare:

```
sudo apt-get install virtinst
```

Durante l'uso di virt-install sono disponibili molte azioni, per esempio:

```
sudo virt-install -n web_devel -r 256 \ --disk path=/var/lib/libvirt/images/web_devel.img,bus=virti
```

- *-n web_devel*: il nome della nuova macchine virtuale usato in questo esempio sarà *web_devel*.
- *-r 256:*: specifica la quantità di memoria che la macchina virtuale userà, in megabyte.
- *--disk path=/var/lib/libvirt/images/web_devel.img,size=4:*: indica il percorso al disco virtuale che può essere un file, una partizione o un volume logico. In questo esempio è un file chiamato `web_devel.img` nella directory /var/lib/libvirt/images/, con una dimensione di 4 gigabyte, che usa *virtio* come bus del disco.
- *-c jeos.iso*: il file usato come CD-ROM virtuale. Il file può essere un file ISO o il percorso al device del CD-ROM nell'host.
- *--accelerate*: abilita le tecnologie di accelerazione nel kernel.
- *--network* fornisce dettagli sull'interfaccia della rete della VM. Qui è usata la rete *predefinita*, e il modello di interfaccia è configurato per *virtio*.
- *--vnc*: esporta la console virtuale usando VNC.
- *--noautoconsole*: non si collegherà automaticamente alla console della macchina virtuale.
- *-v*: crea un ospite completamente virtualizzato.

[1] https://help.ubuntu.com/12.10/installation-guide/

Una volta lanciata virt-install è possibile collegarsi alla console della macchina virtuale utilizzando, localmente, un'interfaccia grafica oppure l'utilità virt-viewer.

1.4. virt-clone

L'applicazione virt-clone può essere usata per copiare una macchina virtuale in un'altra, per esempio:

```
sudo virt-clone -o web_devel -n database_devel -f /path/to/database_devel.img \ --connect=qemu:///s
```

- *-o*: macchina virtuale originale.
- *-n*: nome della nuova macchina virtuale.
- *-f*: percorso al file, volume logico o partizione da usare per la nuova macchina virtuale.
- *--connect*: specifica a quale hypervisor collegarsi.

Usare anche le opzioni *-d* o *--debug* per risolvere i problemi che potrebbero verificarsi con virt-clone.

Sostituire *web_devel* e *database_devel* con i nomi delle macchine virtuali appropriati.

1.5. Gestire la macchina virtuale

1.5.1. virsh

Sono disponibili diverse utilità per la gestione delle macchine virtuali e di libvirt. L'utilità virsh può essere utilizzata dalla riga di comando. Alcuni esempi:

- Per elencare le macchine virtuali in esecuzione:

```
virsh -c qemu:///system list
```

- Per avviare una macchina virtuale:

```
virsh -c qemu:///system start web_devel
```

- Similmente, per lanciare una macchina virtuale durante l'avvio del computer:

```
virsh -c qemu:///system autostart web_devel
```

- Riavviare una macchina virtuale con:

```
virsh -c qemu:///system reboot web_devel
```

- Lo *stato* di una macchina virtuale può essere salvato in un file per poterlo ripristinare successivamente. Il seguente comando salva lo stato della macchina virtuale in un file nominato in base alla data.

```
virsh -c qemu:///system save web_devel web_devel-022708.state
```

Una volta salvata, la macchina virtuale non sarà più in esecuzione.

- Per ripristinare una macchina virtuale:

```
virsh -c qemu:///system restore web_devel-022708.state
```

- Per arrestare una macchina virtuale:

```
virsh -c qemu:///system shutdown web_devel
```

- Per montare un CD-ROM in una macchina virtuale, digitare:

```
virsh -c qemu:///system attach-disk web_devel /dev/cdrom /media/cdrom
```

Nell'esempio precedente, sostituire *web_devel* con il nome della macchina virtuale appropriata e `web_devel-022708.state` con un nome file descrittivo.

1.5.2. Gestore macchina virtuale

Il pacchetto virt-manager contiene un'utilità grafica per gestire le macchie virtuali locali e remote. Per installare virt-manager digitare:

```
sudo apt-get install virt-manager
```

Dato che virt-manager richiede un'interfaccia grafica (GUI), è raccomandato installarlo su una workstation o una postazione di prova invece che un server di produzione. Per connettersi al servizio libvirt locale:

```
virt-manager -c qemu:///system
```

È possibile collegarsi al servizio libvirt in esecuzione su un altro host digitando, in un terminale:

```
virt-manager -c qemu+ssh://virtnode1.mydomain.com/system
```

L'esempio precedente assume che la connessione SSH tra il sistema di gestione e virtnode1.mydomain.com sia già configurata e utilizzi le chiavi SSH per l'autenticazione. Le *chiavi* SSH sono necessarie perché libvirt invia il prompt password a un altro processo. Per maggiori informazioni sulla configurazione di SSH, consultare la *Sezione 1, «Server OpenSSH» [82]*

1.6. Visualizzatore di macchine virtuali

L'applicazione virt-viewer consente di collegarsi alla console di una macchina virtuale. virt-viewer non richiede un'interfaccia grafica per interagire con la macchina virtuale.

Per installare virt-viewer, da un terminale digitare:

```
sudo apt-get install virt-viewer
```

Una volta installata e in esecuzione, è possibile connettersi alla console della macchina virtuale digitando:

```
virt-viewer -c qemu:///system web_devel
```

Analogamente a virt-manager, virt-viewer può collegarsi a un host remoto utilizzando *SSH* con chiave di autenticazione:

```
virt-viewer -c qemu+ssh://virtnode1.miodominio.it/system web_devel
```

Assicurarsi di sostituire *web_devel* con il nome corretto della macchina virtuale.

Se configurato per usare un'interfaccia di rete *bridged*, è anche possibile impostare accesso SSH alla macchina virtuale. Per maggiori informazioni, consultare *Sezione 1, «Server OpenSSH» [82]* e *Sezione 1.4, «Bridging» [42]*.

1.7. Risorse

- See the *KVM*[2] home page for more details.
- Per maggiori informazioni su libvirt, consultare *il sito web di libvirt*[3]
- Il sito di *Virtual Machine Manager*[4] dispone di ulteriori informazioni riguardo lo sviluppo di virt-manager.
- È anche possibile passare nel canale IRC *#ubuntu-virt* su *freenode*[5] per discutere delle tecnologie di virtualizzazione in Ubuntu.
- Un'altra ottima risorsa è la *documentazione online*[6] riguardo KVM.
- For information on Xen, including using Xen with libvirt, please see the *Ubuntu Wiki Xen*[7] page.

2 http://www.linux-kvm.org/
3 http://libvirt.org/
4 http://virt-manager.et.redhat.com/
5 http://freenode.net/
6 https://help.ubuntu.com/community/KVM
7 https://help.ubuntu.com/community/Xen

2. JeOS e vmbuilder

2.1. Introduzione

2.1.1. Cos'è JeOS

Ubuntu *JeOS* (pronunciato come la parola «juice») è una variante di della versione server di Ubuntu, configurata appositamente per le applicazioni virtuali. Non è disponibile sotto forma di file ISO per CD-ROM, ma solo come opzione:

- durante l'installazione della versione server (premere *F4* alla prima schermata per scegliere l'opzione «Installa un sistema minimale», che equivale a selezionare JeOS).
- oppure può essere generato usando «vmbuilder» come descritto di seguito.

JeOS è un'installazione di Ubuntu Server Edition con un kernel appositamente configurato che contiene gli elementi basilari necessari all'esecuzione di un ambiente virtualizzato.

Ubuntu JeOS è stato progettato per sfruttare tutte quelle tecnologie chiave, relative alle prestazioni, presenti negli ultimi prodotti di virtualizzazione di VMware. La combinazione di una ridotta dimensione e prestazioni ottimizzate, assicurano che Ubuntu JeOS Edition sia in grado di offrire un uso efficiente delle risorse server in grandi produzioni virtuali.

Senza l'utilizzo di driver non necessari e ricorrendo solo ai pacchetti richiesti, gli ISV possono configurare il proprio SO di supporto proprio come desiderano. Inoltre, viene assicurato che gli aggiornamenti, di sicurezza o per miglioramenti, saranno limitati al minimo richiesto dallo specifico ambiente. Gli utenti che sviluppano soluzioni virtuali basate su JeOS, dovranno gestire meno aggiornamenti, e quindi una minor manutenzione, di quanto avrebbero dovuto fare con un'installazione server completa.

2.1.2. Cos'è vmbuilder

Utilizzando vmbuilder non è necessario scaricare un'immagine di JeOS: verranno scaricati i pacchetti necessari per creare una macchina virtuale adatta alle proprie esigenze. vmbuilder è uno script che automatizza la creazione di una macchina virtuale Linux. Gli hypervisor supportati attualmente sono KVM e Xen.

È possibile passare opzioni a riga di comando per aggiungere dei pacchetti, per rimuoverne, per scegliere la versione di Ubuntu, quale mirror, ecc... Su piattaforme hardware recenti dotate di molta memoria RAM, con tmpdir in `/dev/shm` o usando un tmpfs e un mirror locale, è possibile avere una macchina virtuale in meno di un minuto.

Introdotto come semplice script shell in Ubuntu 8.04 LTS, ubuntu-vm-builder era un semplice progetto per aiutare gli sviluppatori nel provare il codice scritto in una virtual machine senza dover ricominciare sempre da capo. Lo script è stato in seguito migliorato e Soren Hansen (l'autore dello script e lo specialista di virtualizzazione in Ubuntu virtualization, non il giocatore di golf) lo ha riscritto da capo per Intrepid in python con i seguenti obiettivi:

- Svilupparlo affinché possa essere usato anche da altre distribuzioni.
- Usare un meccanismo di plugin per tutte le interazioni di virtualizzazione per facilitare l'aggiunta di altri ambienti di virtualizzazione o una logica più complessa.
- Fornire un'interfaccia web facile da usare come opzione alla riga di comando.

I principi generali e i comandi restano sempre gli stessi.

2.2. Configurazione iniziale

Si presuppone che siano già stati installati e configurati libvirt e KVM sul computer che si intende usare. Per maggiori informazioni, consultare:

- *Sezione 1, «libvirt» [311]*
- La pagina relativa a *KVM*[8] nella documentazione (in inglese).

Si dà per assodato che si sappia utilizzare un editor di testo come nano oppure vi. In caso contrario, è possibile avere una panoramica dei vari editor di testo consultando *la documentazione di Ubuntu*[9]. Questa guida è stata scritta basandosi su KVM, ma il principio dovrebbe essere lo stesso anche per altre tecnologie di virtualizzazione.

2.2.1. Installare vmbuilder

Il nome del pacchetto da installare è python-vm-builder. In un terminale digitare:

```
sudo apt-get install python-vm-builder
```

Se si sta eseguendo la versione 8.04 è sempre possibile eseguire queste azioni usando la versione del pacchetto chiamata ubuntu-vm-builder; ci sono solo alcune modifiche nella sintassi da usare con il programma.

2.3. Definire una macchina virtuale

Definire una macchina virtuale con vmbuilder è molto facile, ma è necessario prendere in considerazione alcuni aspetti:

- Se si pianifica di fornire applicativi virtuali, non assumere che l'utente finale sappia come estendere la dimensione del disco secondo le proprie esigenze. Prendere quindi in considerazione l'utilizzo di dischi virtuali di grandi dimensioni per consentire agli applicativi di crescere o spiegare nella documentazione come allocare maggiore spazio. Potrebbe essere una buona idea salvare i dati in un sistema di archiviazione esterno.
- Dato che la memoria RAM è più facile da allocare in una MV, la dimensione della RAM dovrebbe essere impostata a un valore minimo sicuro per la propria applicazione.

---

[8] https://help.ubuntu.com/community/KVM
[9] http://wiki.ubuntu-it.org/Ufficio/EditorDiTesto#powereditor

Il comando vmbuilder dispone di due parametri principali: la *tecnologia di virtualizzazione (hypervisor)* e la *distribuzione* finale. Sono disponibili molti altri parametri e tutti possono essere visualizzati con il seguente comando:

```
vmbuilder kvm ubuntu --help
```

2.3.1. Parametri base

As this example is based on KVM and Ubuntu 12.10 (Quantal Quetzal), and we are likely to rebuild the same virtual machine multiple time, we'll invoke vmbuilder with the following first parameters:

```
sudo vmbuilder kvm ubuntu --suite quantal --flavour virtual --arch i386  \
-o --libvirt qemu:///system
```

Il parametro --*suite* definisce il rilascio di Ubuntu, --*flavour* specifica di usare il kernel virtuale (quello usato per generare un'immagine JeOS), --*arch* indica di usare un computer a 32 bit, -*o* indica a vmbuilder di sovrascrivere la versione precedente della macchina virtuale e --*libvirt* aggiunge la macchina virtuale risultante tra quelle disponibili nell'ambiente di virtualizzazione.

Note:

- Data la natura delle operazioni eseguite da vmbuilder, sono necessari i privilegi di root.
- Se la macchina virtuale necessita di usare più di 3GB di RAM, è utile generare una macchina a 64 bit (--arch amd64).
- Fino a Ubuntu 8.10, il kernel virtuale era generato solo per architetture a 32 bit, per definire quindi una macchina amd64 su Hardy, usare --*flavour server*.

2.3.2. Parametri di installazione di JeOS

2.3.2.1. Rete con JeOS

2.3.2.1.1. Assegnare un indirizzo IP fisso

Come applicazione che verrà messa in produzione all'interno di reti diverse, è molto difficile conoscere la struttura attuale della rete. Per semplificare la configurazione è utile procedere come solitamente procedono i venditori di hardware di rete, assegnando un indirizzo IP fisso all'interno di una classe di rete che verrà descritta all'interno della propria documentazione. Un indirizzo nell'intervallo 192.168.0.0/255 è una buona scelta.

Per ottenere questo vengono usati i seguenti parametri:

- --*ip INDIRIZZO*: indirizzo IP (il valore predefinito è dhcp se non viene specificato nulla)
- --*hostname NOME*: impostare il nome host dell'ospite.
- --*mask VALORE*: maschera di rete (valore predefinito: 255.255.255.0)
- --*net VALORE*: indirizzo IP net (valore predefinito: X.X.X.0)
- --*bcast VALORE*: broadcast (valore predefinito: X.X.X.255)

- *--gw INDIRIZZO*: indirizzo del gateway (valore predefinito: X.X.X.1)
- *--dns INDIRIZZO*: indirizzo server dei nomi (valore predefinito: X.X.X.1)

Si dà per scontato che i valori predefiniti siano sufficienti. Il comando diventa:

```
sudo vmbuilder kvm ubuntu --suite quantal --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm
```

2.3.2.1.2. Bridging

Considerato che host remoti dovranno avere accesso all'applicazione, è necessario configurare libvirt in modo tale che questa utilizzi la rete in modalità bridge; per ottenere questo risultato, aggiungere l'opzione *--bridge* al comando:

```
sudo vmbuilder kvm ubuntu --suite quantal --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm --bridge br0
```

È necessario configurare preliminarmente un'interfaccia bridge, consultare *Sezione 1.4, «Bridging» [42]* per ulteriori informazioni. Inoltre, se il nome dell'interfaccia è diverso, modificare *br0* nell'interfaccia bridge.

2.3.2.2. Partizionamento

Il partizionamento dell'applicativo virtuale deve prendere in considerazione cosa si intende fare. Dato che molti applicativi non avranno un sistema di archiviazione separato per i dati, usare una partizione `/var` separata è una buona idea.

Per ottenere tutto questo, vmbuilder dispone dell'opzione *--part*:

```
--part PATH
  Allows you to specify a partition table in a partition file, located at PATH. Each
  line of the partition file should specify (root first):
      mountpoint size
  where size is in megabytes. You can have up to 4 virtual disks, a new disk starts
  on a line with '---'. ie :
      root 1000
      /opt 1000
      swap 256
      ---
      /var 2000
      /log 1500
```

In questo caso, creare un file di testo `vmbuilder.partition` contenente quanto segue:

```
root 8000
swap 4000
---
```

```
/var 20000
```

Notare che vengono usate immagini disco virtuali, le dimensioni inserite sono le dimensioni massime dei volumi.

Il comando diventa quindi:

```
sudo vmbuilder kvm ubuntu --suite quantal --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm --part vmbuilder.partition
```

L'uso di «\» all'interno di un comando consente di scrivere comandi su più righe.

2.3.2.3. Utente e password

È necessario anche impostare un utente e una password predefiniti e generici da poter includere nella documentazione. Successivamente verrà presentato uno script che viene eseguito al primo accesso di un utente che tra le molte cose chiederà di modificare la password. In questo esempio viene usato come nome utente *user* e *default* come password.

Per fare questo vengono usati i seguenti parametri:

- *--user NOME_UTENTE*: imposta il nome utente da aggiungere. Valore predefinito: ubuntu.
- *--name NOME_COMPLETO*: imposta il nome completo dell'utente da aggiungere. Valore predefinito: Ubuntu.
- *--pass PASSWORD*: imposta la password dell'utente: Valore predefinito: ubuntu.

Il comando ora è il seguente:

```
sudo vmbuilder kvm ubuntu --suite quantal --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm --part \
vmbuilder.partition --user user --name user --pass default
```

2.3.3. Installare i pacchetti richiesti

In questo esempio verrà installato un pacchetto (Limesurvey) che accede a un database MySQL ed è dotato di un'interfaccia web. Il sistema operativo dovrà quindi aver installato:

- Apache
- PHP
- MySQL
- Server OpenSSH
- Limesurvey (un'applicazione di esempio creata appositamente)

Questo è ottenuto usando vmbuilder specificando l'opzione --addpkg diverse volte:

```
--addpkg PKG
  Install PKG into the guest (can be specfied multiple times)
```

Purtroppo, in base al funzionamento di vmbuilder, i pacchetti che devono porre delle domande nella fase di post-installazione non sono supportati e dovrebbero essere installati successivamente quando è possibile interagirvi. Questo è il caso di Limesurvey che verrà installato successivamente, dopo che l'utente ha eseguito l'accesso.

Altri pacchetti che pongono delle semplici domande di debconf, come mysql-server che richiede di impostare una password, possono essere installati, ma dovranno essere riconfigurati una volta eseguito l'accesso.

Se alcuni dei pacchetti che si devono installare non sono presenti nel componente «main», è necessario abilitare dei repository aggiuntivi usando le opzioni «--comp» e «--ppa»:

```
--components COMP1,COMP2,...,COMPN
           A comma separated list of distro components to include (e.g. main,universe).
           This defaults to "main"
--ppa=PPA Add ppa belonging to PPA to the vm's sources.list.
```

Limesurvey non fa parte degli archivi attualmente ed è quindi necessario specificarne l'indirizzo PPA (Personal Package Archive) così da aggiungerlo al file `/etc/apt/source.list` della macchina virtuale. Aggiungere quindi quanto segue al comando:

```
--addpkg apache2 --addpkg apache2-mpm-prefork --addpkg apache2-utils \ --addpkg apache2.2-common --
```

2.3.4. Considerazioni sulla velocità

2.3.4.1. Cache dei pacchetti

Quando vmbuilder genera il sistema, necessita di scaricare dai repository in rete ogni singolo pacchetto di cui il sistema è composto e questo, in base alla velocità della connessione e al carico del mirror, può avere un forte impatto sui tempi di generazione. Per ridurre questo effetto, è utile avere un repository locale (che è possibile creare usando apt-mirror) o un proxy cache come apt-proxy. La seconda opzione, descritta di seguito, è quella più facile da implementare e richiede meno spazio su disco. Per installare il tutto, digitare:

```
sudo apt-get install apt-proxy
```

Una volta completata l'installazione, il proxy (vuoto) è pronto all'indirizzo «http://INDIRIZZO_MIRROR:9999» e troverà i repository Ubuntu sotto «/ubuntu». Affinché vmbuilder possa usarlo, è necessario usare l'opzione --*mirror*:

```
--mirror=URL  Use Ubuntu mirror at URL instead of the default, which
              is http://archive.ubuntu.com/ubuntu for official
              arches and http://ports.ubuntu.com/ubuntu-ports
```

```
              otherwise
```

Aggiungere quindi al comando:

```
--mirror http://INDIRIZZO_MIRROR:9999/ubuntu
```

L'indirizzo del mirror qui specificato verrà usato anche nel file `/etc/apt/sources.list` del nuovo ospite creato, ed è pertanto utile specificare un indirizzo che può essere utilizzato dall'ospite oppure pianificare una modifica dell'indirizzo in un secondo momento.

2.3.4.2. Installare un mirror locale

Se si è in un ambiente molto grande, può aver senso creare un mirror locale dei repository di Ubuntu. Il pacchetto «apt-mirror» fornisce uno script per la gestione delle operazioni di mirror. È utile avere almeno 20GB di spazio per ogni rilascio supportato e architettura.

Per impostazione predefinita, apt-mirror usa il file di configurazione `/etc/apt/mirror.list`; dato che è già impostato, dovrà solamente replicare l'architettura del computer locale. Se è necessario supportare altre architetture all'interno del mirror, basta duplicare le righe che iniziano con «deb», sostituendo la parola «deb» con «/deb-{arch}», dove «arch» può essere i386, amd64, ecc... Per esempio, su architettura amd64, per avere anche gli archivi per i386, si avrà (alcune righe sono state divise per adattarle al formato di questo documento):

```
deb  http://archive.ubuntu.com/ubuntu quantal main restricted universe multiverse
/deb-i386  http://archive.ubuntu.com/ubuntu quantal main restricted universe multiverse

deb  http://archive.ubuntu.com/ubuntu quantal-updates main restricted universe multiverse
/deb-i386  http://archive.ubuntu.com/ubuntu quantal-updates main
 restricted universe multiverse

deb http://archive.ubuntu.com/ubuntu/ quantal-backports main restricted universe multiverse
/deb-i386  http://archive.ubuntu.com/ubuntu quantal-backports main
 restricted universe multiverse

deb http://security.ubuntu.com/ubuntu quantal-security main restricted universe multiverse
/deb-i386  http://security.ubuntu.com/ubuntu quantal-security main
 restricted universe multiverse

deb http://archive.ubuntu.com/ubuntu quantal main/debian-installer
 restricted/debian-installer universe/debian-installer multiverse/debian-installer
/deb-i386 http://archive.ubuntu.com/ubuntu quantal main/debian-installer
 restricted/debian-installer universe/debian-installer multiverse/debian-installer
```

I pacchetti dei sorgenti non sono stati inclusi nel mirror dato che non sono molto usati quanto i binari e occupano molto spazio. È comunque possibile aggiungerli facilmente all'elenco.

Una volta terminata l'operazione di duplicazione del mirror (può durare molto), è necessario configurare Apache affinché i file del mirror (in `/var/spool/apt-mirror` se non è stato modificato il

valore predefinito) siano pubblicati dal proprio server Apache. Per maggiori informazioni su Apache, consultare *Sezione 1, «HTTPD - Server web Apache2» [188]*.

2.4. Pacchettizzare l'applicativo

Sono disponibili due opzioni:

- Il metodo raccomandato è quello di creare un pacchetto *Debian*. Dato che questo argomento esula da questa guida, non verrà spiegato questo metodo e si rimanda alla *Ubuntu Packaging Guide*[10]. In questo caso è anche utile creare un repository per contenere il pacchetto in modo tale che gli aggiornamenti vengano prelevati da questo. Per ulteriori informazioni, consultare *Debian Administration*[11].
- Installare l'applicativo nella directory `/opt` come raccomandato dalle *linee guida di FHS*[12].

In questo caso viene usato Limesurvey come esempio di applicazione web per cui creare un applicativo virtuale. Come accennato precedentemente. è disponibile un pacchetto di questa applicazione attraverso gli archivi PPA (Personal Package Archive).

2.5. Utili accorgimenti

2.5.1. Configurare gli aggiornamenti automatici

Affinché il sistema sia configurato per aggiornarsi automaticamente a scadenze determinate, basta installare il pacchetto unattended-upgrades. Aggiungere quindi quanto segue al comando:

```
--addpkg unattended-upgrades
```

Dato che il pacchetto dell'applicazione è stata inserito nel PPA, il processo di aggiornamento non aggiornerà solamente il sistema, ma anche l'applicazione ogni qualvolta ci sia una versione aggiornata nel PPA.

2.5.2. Gestire gli eventi ACPI

Affinché la macchina virtuale possa gestire gli eventi come riavvio e arresto che le vengono inviati, è utile installare anche il pacchetto «acpid». Aggiungere quindi quanto segue al comando:

```
--addpkg acpid
```

2.6. Il comando finale

Ecco il comando con tutte le opzioni presentate poco sopra:

[10] https://wiki.ubuntu.com/PackagingGuide
[11] http://www.debian-administration.org/articles/286
[12] http://www.pathname.com/fhs/

```
sudo vmbuilder kvm ubuntu --suite quantal --flavour virtual --arch i386 -o \
         --libvirt qemu:///system --ip 192.168.0.100 --hostname myvm \
         --part vmbuilder.partition --user user --name user --pass default \
         --addpkg apache2 --addpkg apache2-mpm-prefork --addpkg apache2-utils \
         --addpkg apache2.2-common --addpkg dbconfig-common \
         --addpkg libapache2-mod-php5 --addpkg mysql-client --addpkg php5-cli \
         --addpkg php5-gd --addpkg php5-ldap --addpkg php5-mysql \
         --addpkg wwwconfig-common --addpkg mysql-server \
         --addpkg unattended-upgrades --addpkg acpid --ppa nijaba \
         --mirror http://mirroraddress:9999/ubuntu
```

2.7. Risorse

Per avere maggiori informazioni, per porre qualche domanda o per lasciare dei suggerimenti, contattare l'«Ubuntu Server Team» presso:

- IRC: #ubuntu-server on freenode
- Mailing list: *ubuntu-server at lists.ubuntu.com*[13]
- Consultare anche la pagina *della documentazione della comunità su JeOSVMBuilder*[14]

[13] https://lists.ubuntu.com/mailman/listinfo/ubuntu-server
[14] https://help.ubuntu.com/community/JeOSVMBuilder

3. Ubuntu Cloud

Cloud computing is a computing model that allows vast pools of resources to be allocated on-demand. These resources such as storage, computing power, network and software are abstracted and delivered as a service over the Internet anywhere, anytime. These services are billed per time consumed similar to the ones used by public services such as electricity, water and telephony. Ubuntu Cloud Infrastructure uses OpenStack open source software to help build highly scalable, cloud computing for both public and private clouds.

3.1. Panoramica

This tutorial covers the OpenStack installation from the Ubuntu 12.10 Server Edition CD, and assumes a basic network topology, with a single system serving as the "all-in-one cloud infrastructure".Due to the tutorial's simplicity, the instructions as-is are not intended to set up production servers although it allows you to have a POC (proof of concept) of the Ubuntu Cloud using OpenStack.

3.2. Prerequisiti

To deploy a minimal Ubuntu Cloud infrastructure, you'll need at least:

- One dedicated system.
- Two network address ranges (private network and public network).
- Make sure the host in question supports VT (Virtualization Technology) since we will be using KVM as the virtualization technology. Other hypervisors are also supported such as QEMU, UML, Vmware ESX/ESXi and XEN. LXC (Linux Containers) is also supported through libvirt.

  Check if your system supports kvm issuing **sudo kvm-ok** in a linux terminal.

The **"Minimum Topology"** recommended for production use is using three nodes **-** One master server running nova services (except compute) and two servers running nova-compute. This setup is not redundant and the master server is a SPoF (Single Point of Failure).

3.3. Preconfiguring the network

Before we start installing OpenStack we need to make sure we have bridging support installed, a MySQL database, and a central time server (ntp). This will assure that we have instantiated machines and hosts in sync.

In this example the "private network" will be in the 10.0.0.0/24 range on eth1. All the internal communication between instances will happen there while the "public network" will be in the 10.153.107.0/29 range on eth0.

3.3.1. Install bridging support

```
sudo apt-get install bridge-utils
```

3.3.2. Install and configure NTP

```
sudo apt-get install ntp
```

Add these two lines at the end of the `/etc/ntp.conf` file.

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
```

Restart ntp service

```
sudo service ntp restart
```

3.3.3. Install and configure MySQL

```
sudo apt-get install mysql-server
```

Create a database and mysql user for OpenStack

```
sudo mysql -uroot -ppassword -e "CREATE DATABASE nova;"
sudo mysql -uroot -ppassword -e "GRANT ALL ON nova.* TO novauser@localhost \
IDENTIFIED BY 'novapassword' ";
```

The line continuation character "\" implies that you must include the subsequent line as part of the current command.

3.4. Install OpenStack Compute (Nova)

OpenStack Compute (Nova) is a cloud computing fabric controller (the main part of an IaaS system). It is written in Python, using the Eventlet and Twisted frameworks, and relies on the standard AMQP messaging protocol, and SQLAlchemy for data store access.

Install OpenStack Nova components

```
sudo apt-get install nova-api nova-network nova-volume nova-objectstore nova-scheduler \
nova-compute euca2ools unzip
```

Restart libvirt-bin just to make sure libvirtd is aware of ebtables.

```
sudo service libvirt-bin restart
```

Install RabbitMQ – Advanced Message Queuing Protocol (AMQP)

```
sudo apt-get install rabbitmq-server
```

Edit `/etc/nova/nova.conf` and add the following:

```
# Nova config FlatDHCPManager
--sql_connection=mysql://novauser:novapassword@localhost/nova
--flat_injected=true
--network_manager=nova.network.manager.FlatDHCPManager
--fixed_range=10.0.0.0/24
--floating_range=10.153.107.72/29
--flat_network_dhcp_start=10.0.0.2
--flat_network_bridge=br100
--flat_interface=eth1
--public_interface=eth0
```

Restart OpenStack services

```
for i in nova-api nova-network nova-objectstore nova-scheduler nova-volume nova-compute; \
do sudo stop $i; sleep 2; done
```

```
for i in nova-api nova-network nova-objectstore nova-scheduler nova-volume nova-compute; \
do sudo start $i; sleep 2; done
```

Migrate Nova database from sqlite db to MySQL db. It may take a while.

```
sudo nova-manage db sync
```

Define a specific private network where all your Instances will run. This will be used in the network of fixed Ips set inside `nova.conf` .

```
sudo nova-manage network create --fixed_range_v4 10.0.0.0/24 --label private \
--bridge_interface br100
```

Define a specific public network and allocate 6 (usable) Floating Public IP addresses for use with the instances starting from 10.153.107.72.

```
sudo nova-manage floating create --ip_range=10.153.107.72/29
```

Create a user (user1), a project (project1), download credentials and source its configuration file.

```
cd ; mkdir nova ; cd nova
sudo nova-manage user admin user1
sudo nova-manage project create project1 user1
sudo nova-manage project zipfile project1 user1
unzip nova.zip
source novarc
```

Verify the OpenStack Compute installation by typing:

```
sudo nova-manage service list
sudo nova-manage version list
```

If nova services don’t show up correctly restart OpenStack services as described previously. For more information please refer to the troubleshooting section on this guide.

3.5. Install Imaging Service (Glance)

Nova uses Glance service to manage Operating System images that it needs for bringing up instances. Glance can use several types of storage backends such as filestore, s3 etc. Glance has two components - *glance-api and glance-registry*. These can be controlled using the concerned upstart service jobs. For this specific case we will be using mysql as a storage backend.

Install Glance

```
sudo apt-get install glance
```

Create a database and user for glance

```
sudo mysql -uroot -ppassword -e "CREATE DATABASE glance;"
sudo mysql -uroot -ppassword -e "GRANT ALL ON glance.* TO glanceuser@localhost \
IDENTIFIED BY 'glancepassword' ";
```

Edit the file /etc/glance/glance-registry.conf and edit the line which contains the option "sql_connection =" to this:

```
sql_connection = mysql://glanceuser:glancepassword@localhost/glance
```

Remove the sqlite database

```
rm -rf /var/lib/glance/glance.sqlite
```

Restart glance-registry after making changes to /etc/glance/glance-registry.conf. The MySQL database will be automatically populated.

```
sudo restart glance-registry
```

If you find issues take a look at the log file in /var/log/glance/api.log and /var/log/glance/registry.log.

3.6. Running Instances

Before you can instantiate images, you first need to setup user credentials. Once this first step is achieved you also need to upload images that you want to run in the cloud. Once you have these images uploaded to the cloud you will be able to run and connect to them. Here are the steps you should follow to get OpenStack Nova running instances:

Download, register and publish an Ubuntu cloud image

```
distro=lucid
wget http://cloud-images.ubuntu.com/$distro/current/$distro-server-cloudimg-amd64.tar.gz
cloud-publish-tarball "$distro"-server-cloudimg-amd64.tar.gz "$distro"_amd64
```

Create a key pair and start an instance

```
cd ~/nova
source novarc
euca-add-keypair user1 > user1.priv
chmod 0600 user1.priv
```

Allow icmp (ping) and ssh access to instances

```
euca-authorize default -P tcp -p 22 -s 0.0.0.0/0
euca-authorize -P icmp -t -1:-1 default
```

Run an instance

```
ami=`euca-describe-images |  awk {'print $2'} | grep -m1 ami`
euca-run-instances $ami -k user1 -t m1.tiny
euca-describe-instances
```

Assign public address to the instance.

```
euca-allocate-address
euca-associate-address -i instance_id public_ip_address
euca-describe-instances
```

You must enter above the instance_id (ami) and public_ip_address shown above by euca-describe-instances and euca-allocate-address commands.

Now you should be able to SSH to the instance

```
ssh -i user1.priv ubuntu@ipaddress
```

To terminate instances

```
euca-terminate-instances instance_id
```

3.7. Install the Storage Infrastructure (Swift)

Swift is a highly available, distributed, eventually consistent object/blob store. It is used by the OpenStack Infrastructure to provide S3 like cloud storage services. It is also S3 api compatible with amazon.

Organizations use Swift to store lots of data efficiently, safely, and cheaply where applications use an special api to interface between the applications and objects stored in Swift.

Although you can install Swift on a single server, a multiple-server installation is required for production environments. If you want to install OpenStack Object Storage (Swift) on a single node for development or testing purposes, use the Swift All In One instructions on Ubuntu.

For more information see: *http://swift.openstack.org/development_saio.html* [15] .

3.8. Support and Troubleshooting

Community Support

- *OpenStack Mailing list*[16]
- *The OpenStack Wiki search*[17]
- *Launchpad bugs area*[18]
- Join the IRC channel #openstack on freenode.

3.9. Risorse

- *Cloud Computing - Service models*[19]
- *OpenStack Compute*[20]
- *OpenStack Image Service*[21]
- *OpenStack Object Storage Administration Guide*
- *Installing OpenStack Object Storage on Ubuntu*[22]
- *http://cloudglossary.com/*

3.10. Glossario

The Ubuntu Cloud documentation uses terminology that might be unfamiliar to some readers. This page is intended to provide a glossary of such terms and acronyms.

- *Cloud* - A federated set of physical machines that offer computing resources through virtual machines, provisioned and recollected dynamically.
- *IaaS* - Infrastructure as a Service — Cloud infrastructure services, whereby a virtualized environment is delivered as a service over the Internet by the provider. The infrastructure can include servers, network equipment, and software.

[15] http://swift.openstack.org/development_saio.html
[16] https://launchpad.net/~openstack
[17] http://wiki.openstack.org
[18] https://bugs.launchpad.net/nova
[19] http://en.wikipedia.org/wiki/Cloud_computing#Service_Models
[20] docs.openstack.org/trunk/openstack-compute/
[21] http://docs.openstack.org/diablo/openstack-compute/starter/content/GlanceMS-d2s21.html
[22] http://docs.openstack.org/trunk/openstack-object-storage/admin/content/installing-openstack-object-storage-on-ubuntu.html

- *EBS* - Elastic Block Storage.
- *EC2* - Elastic Compute Cloud. Amazon's pay-by-the-hour, pay-by-the-gigabyte public cloud computing offering.
- *Node* - A node is a physical machine that's capable of running virtual machines, running a node controller. Within Ubuntu, this generally means that the CPU has VT extensions, and can run the KVM hypervisor.
- *S3* - Simple Storage Service. Amazon's pay-by-the-gigabyte persistent storage solution for EC2.
- *Ubuntu Cloud* - Ubuntu Cloud. Ubuntu's cloud computing solution, based on OpenStack.
- *VM* - Virtual Machine.
- *VT* - Virtualization Technology. An optional feature of some modern CPUs, allowing for accelerated virtual machine hosting.

4. LXC

I contenitori sono una tecnologia leggera di virtualizzazione; sono più simili a un chroot avanzato che a una virtualizzazione completa come Qemu o VMware, in quanto non emulano le componenti hardware e condividono il medesimo sistema operativo dell'host. I contenitori possono pertanto essere più propriamente comparati alle zone Solaris o alle jail BSD. Linux-vserver e OpenVZ sono due implementazioni pre-esistenti, sviluppate in maniera indipendente, di funzionalità del tipo contenitore per Linux. In effetti i contenitori hanno avuto origine dal lavoro in upstream delle funzionalità vserver e OpenVZ. Alcune delle funzionalità di vserver e OpenVZ sono ancora assenti nei contenitori, che tuttavia sono in grado di effettuare l'*avvio* di molte distribuzioni Linux e hanno il vantaggio di poter essere utilizzati con un kernel non modificato upstream.

Esistono due implementazioni di contenitori spazio utente, ognuna delle quali sfrutta le medesime caratteristiche del kernel. Libvirt consente l'uso di contenitori tramite il driver LXC con connessione a «lxc:///»; può essere molto conveniente, in quanto supporta la stessa sintassi di altri driver. L'altra implementazione, chiamata semplicemente «LXC», non è compatibile con libvirt, ma è più flessibile e offre un maggior numero di strumenti spazio utente. È possibile passare da una implementazione all'altra, sebbene ci siano delle peculiarità che possono ingenerare confusione.

In questo documento verrà illustrato principalmente il pacchetto lxc; verso la fine, si illustrerà l'uso del driver libvirt LXC.

In questo documento il nome di un contenitore sarà indicato come CN, C1 o C2.

4.1. Installazione

Il pacchetto lxc può essere installato usando

```
sudo apt-get install lxc
```

Questo richiamerà le dipendenze necessarie e consigliate, inclusi cgroup-lite, lvm2 e debootstrap. Per usare libvirt-lxc, installare libvirt-bin. LXC e libvirt-lxc possono essere installati e usati allo stesso tempo.

4.2. Impostazione dell'host

4.2.1. Impostazione di base dei file LXC

Segue una descrizione dei file e delle directory installate e utilizzate da LXC.

- There are two upstart jobs:
  - `/etc/init/lxc-net.conf`: is an optional job which only runs if `/etc/default/lxc` specifies USE_LXC_BRIDGE (true by default). It sets up a NATed bridge for containers to use.
  - `/etc/init/lxc.conf`: runs if LXC_AUTO (true by default) is set to true in `/etc/default/lxc`. It looks for entries under `/etc/lxc/auto/` which are symbolic links to configuration files for the containers which should be started at boot.

- `/etc/lxc/lxc.conf`: Si tratta di un file di configurazione predefinito per la creazione di contenitori, `/etc/lxc/lxc.conf`, che indirizza i contenitori a usare il bridge LXC creato dall'attività upstart lxc-net. Se non viene specificato nessun file di configurazione durante la creazione del contenitore, sarà utilizzato questo file.
- In `/usr/share/doc/lxc/examples` possono essere trovati altri esempi di file di configurazione di contenitori. Questi esempi mostrano come creare contenitori senza una rete locale o usando macvlan, vlan o altre disposizioni di rete.
- I vari strumenti di amministrazione per contenitori sono in `/usr/bin`.
- `/usr/lib/lxc/lxc-init` is a very minimal and lightweight init binary which is used by lxc-execute. Rather than `booting' a full container, it manually mounts a few filesystems, especially `/proc`, and executes its arguments. You are not likely to need to manually refer to this file.
- `/usr/lib/lxc/templates/` contiene i «modelli» da usare per creare nuovi contenitori di svariati tipi per diverse distribuzioni.
- `/etc/apparmor.d/lxc/lxc-default` contiene la politica predefinita Apparmor MAC il cui scopo è proteggere l'host dai contenitori. Per ulteriori informazioni, consultare *Sezione 4.2.6, «Apparmor» [334]*.
- `/etc/apparmor.d/usr.bin.lxc-start` contiene un profilo per proteggere l'host da **lxc-start** mentre viene impostato il contenitore.
- `/etc/apparmor.d/lxc-containers` causes all the profiles defined under `/etc/apparmor.d/lxc` to be loaded at boot.
- Ci sono diverse pagine di manuale per gli strumenti di amministrazione LXC e per il file di configurazione di contenitori `lxc.conf`.
- `/var/lib/lxc` is where containers and their configuration information are stored.
- `/var/cache/lxc` is where caches of distribution data are stored to speed up multiple container creations.

4.2.2. lxcbr0

When USE_LXC_BRIDGE is set to true in /etc/default/lxc (as it is by default), a bridge called lxcbr0 is created at startup. This bridge is given the private address 10.0.3.1, and containers using this bridge will have a 10.0.3.0/24 address. A dnsmasq instance is run listening on that bridge, so if another dnsmasq has bound all interfaces before the lxc-net upstart job runs, lxc-net will fail to start and lxcbr0 will not exist.

Se esiste un altro bridge - il virbr0 predefinito di libvirt o un bridge br0 della NIC predefinita - è possibile usarlo al posto di lxcbr0 per i propri contenitori.

4.2.3. Usare un file system separato per la memorizzazione dei contenitori

LXC stores container information and (with the default backing store) root filesystems under `/var/lib/lxc`. Container creation templates also tend to store cached distribution information under `/var/cache/lxc`.

If you wish to use another filesystem than `/var`, you can mount a filesystem which has more space into those locations. If you have a disk dedicated for this, you can simply mount it at `/var/lib/lxc`. If you'd like to use another location, like `/srv`, you can bind mount it or use a symbolic link. For instance, if `/srv` is a large mounted filesystem, create and symlink two directories:

```
sudo mkdir /srv/lxclib /srv/lxccache sudo rm -rf /var/lib/lxc /var/cache/lxc sudo ln -s /srv/lxclib
```

or, using bind mounts:

```
sudo mkdir /srv/lxclib /srv/lxccache sudo sed -i '$a \ /srv/lxclib /var/lib/lxc none defaults,bind
```

4.2.4. Contenitori integrati con lvm

It is possible to use LVM partitions as the backing stores for containers. Advantages of this include flexibility in storage management and fast container cloning. The tools default to using a VG (volume group) named *lxc*, but another VG can be used through command line options. When a LV is used as a container backing store, the container's configuration file is still `/var/lib/lxc/CN/config`, but the root fs entry in that file (*lxc.rootfs*) will point to the lV block device name, i.e. `/dev/lxc/CN`.

Containers with directory tree and LVM backing stores can co-exist.

4.2.5. Btrfs

If your host has a btrfs `/var`, the LXC administration tools will detect this and automatically exploit it by cloning containers using btrfs snapshots.

4.2.6. Apparmor

LXC è dotato di un profilo Apparmor che protegge l'host da usi impropri accidentali dei privilegi all'interno di un contenitore. Per esempio, il contenitore non può modificare `/proc/sysrq-trigger` o la maggior parte dei file `/sys`.

Il profilo `usr.bin.lxc-start` è eseguito utilizzando **lxc-start**. Questo profilo impedisce a **lxc-start** di montare nuovi file system oltre a quello root del contenitore. Prima di eseguire l'**init** del contenitore, **LXC** richiede di passare al profilo del contenitore; per impostazione predefinita, questo profilo è la politica `lxc-container-default` definita in `/etc/apparmor.d/lxc/lxc-default`. Questo profilo impedisce al contenitore di accedere a molti percorsi pericolosi e di montare la maggior parte dei file system.

Se **lxc-start** si interrompe in quanto la sua politica Apparmor nega un accesso legittimo, è possibile disabilitare il profilo lxc-start eseguendo:

```
sudo apparmor_parser -R /etc/apparmor.d/usr.bin.lxc-start
sudo ln -s /etc/apparmor.d/usr.bin.lxc-start /etc/apparmor.d/disabled/
```

Questo consente l'esecuzione senza restrizioni di **lxc-start**, ma continua a regolare il contenitore stesso; se è necessario eliminare anche le restrizioni del contenitore, oltre a disabilitare il profilo `usr.bin.lxc-start`, occorre aggiungere:

```
lxc.aa_profile = unconfined
```

to the container's configuration file. If you wish to run a container in a custom profile, you can create a new profile under `/etc/apparmor.d/lxc/`. Its name must start with `lxc-` in order for **lxc-start** to be allowed to transition to that profile. The `lxc-default` profile includes the re-usable abstractions file `/etc/apparmor.d/abstractions/lxc/container-base`. An easy way to start a new profile therefore is to do the same, then add extra permissions at the bottom of your policy.

After creating the policy, load it using:

```
sudo apparmor_parser -r /etc/apparmor.d/lxc-containers
```

Il profilo verrà automaticamente caricato dopo un riavvio, perchè è collegato al file `/etc/apparmor.d/lxc-containers`. Infine, per far usare al contenitore `CN` questo nuovo `lxc-CN-profile`, aggiungere la seguente riga al suo file di configurazione:

```
lxc.aa_profile = lxc-CN-profile
```

lxc-execute non immette un profilo Apparmor, ma il contenitore che viene generato sarà limitato.

4.2.7. Control Groups

Control groups (cgroups) are a kernel feature providing hierarchical task grouping and per-cgroup resource accounting and limits. They are used in containers to limit block and character device access and to freeze (suspend) containers. They can be further used to limit memory use and block i/o, guarantee minimum cpu shares, and to lock containers to specific cpus. By default, LXC depends on the cgroup-lite package to be installed, which provides the proper cgroup initialization at boot. The cgroup-lite package mounts each cgroup subsystem separately under `/sys/fs/cgroup/SS`, where SS is the subsystem name. For instance the freezer subsystem is mounted under `/sys/fs/cgroup/freezer`. LXC cgroup are kept under `/sys/fs/cgroup/SS/INIT/lxc`, where INIT is the init task's cgroup. This is `/` by default, so in the end the freezer cgroup for container CN would be `/sys/fs/cgroup/freezer/lxc/CN`.

4.2.8. Privilegi

The container administration tools must be run with root user privilege. A utility called `lxc-setup` was written with the intention of providing the tools with the needed file capabilities to allow non-root users to run the tools with sufficient privilege. However, as root in a container cannot yet be reliably contained, this is not worthwhile. It is therefore recommended to not use `lxc-setup`, and to provide the LXC administrators the needed sudo privilege.

The user namespace, which is expected to be available in the next Long Term Support (LTS) release, will allow containment of the container root user, as well as reduce the amount of privilege required for creating and administering containers.

4.2.9. LXC Upstart Jobs

As listed above, the lxc package includes two upstart jobs. The first, `lxc-net`, is always started when the other, `lxc`, is about to begin, and stops when it stops. If the USE_LXC_BRIDGE variable is set to false in `/etc/defaults/lxc`, then it will immediately exit. If it is true, and an error occurs bringing up the LXC bridge, then the `lxc` job will not start. `lxc-net` will bring down the LXC bridge when stopped, unless a container is running which is using that bridge.

The `lxc` job starts on runlevel 2-5. If the LXC_AUTO variable is set to true, then it will look under `/etc/lxc` for containers which should be started automatically. When the `lxc` job is stopped, either manually or by entering runlevel 0, 1, or 6, it will stop those containers.

To register a container to start automatically, create a symbolic link `/etc/default/lxc/name.conf` pointing to the container's config file. For instance, the configuration file for a container `CN` is `/var/lib/lxc/CN/config`. To make that container auto-start, use the command:

```
sudo ln -s /var/lib/lxc/CN/config /etc/lxc/auto/CN.conf
```

4.3. Container Administration

4.3.1. Creating Containers

The easiest way to create containers is using **lxc-create**. This script uses distribution-specific templates under `/usr/lib/lxc/templates/` to set up container-friendly chroots under `/var/lib/lxc/CN/rootfs`, and initialize the configuration in `/var/lib/lxc/CN/fstab` and `/var/lib/lxc/CN/config`, where CN is the container name

The simplest container creation command would look like:

```
sudo lxc-create -t ubuntu -n CN
```

This tells lxc-create to use the ubuntu template (-t ubuntu) and to call the container CN (-n CN). Since no configuration file was specified (which would have been done with `-f file'), it will use the default configuration file under `/etc/lxc/lxc.conf`. This gives the container a single veth network interface attached to the lxcbr0 bridge.

The container creation templates can also accept arguments. These can be listed after --. For instance

```
sudo lxc-create -t ubuntu -n oneiric1 -- -r oneiric
```

passes the arguments '-r oneiric1' to the ubuntu template.

4.3.1.1. Help

Help on the lxc-create command can be seen by using **lxc-create -h**. However, the templates also take their own options. If you do

```
sudo lxc-create -t ubuntu -h
```

then the general **lxc-create** help will be followed by help output specific to the ubuntu template. If no template is specified, then only help for **lxc-create** itself will be shown.

4.3.1.2. Ubuntu template

The ubuntu template can be used to create Ubuntu system containers with any release at least as new as 10.04 LTS. It uses debootstrap to create a cached container filesystem which gets copied into place each time a container is created. The cached image is saved and only re-generated when you create a container using the *-F* (flush) option to the template, i.e.:

```
sudo lxc-create -t ubuntu -n CN -- -F
```

The Ubuntu release installed by the template will be the same as that on the host, unless otherwise specified with the *-r* option, i.e.

```
sudo lxc-create -t ubuntu -n CN -- -r lucid
```

If you want to create a 32-bit container on a 64-bit host, pass *-a i386* to the container. If you have the qemu-user-static package installed, then you can create a container using any architecture supported by qemu-user-static.

The container will have a user named *ubuntu* whose password is *ubuntu* and who is a member of the *sudo* group. If you wish to inject a public ssh key for the *ubuntu* user, you can do so with *-S sshkey.pub*.

You can also *bind* user jdoe from the host into the container using the *-b jdoe* option. This will copy jdoe's password and shadow entries into the container, make sure his default group and shell are

available, add him to the sudo group, and bind-mount his home directory into the container when the container is started.

When a container is created, the `release-updates` archive is added to the container's `sources.list`, and its package archive will be updated. If the container release is older than 12.04 LTS, then the lxcguest package will be automatically installed. Alternatively, if the *--trim* option is specified, then the lxcguest package will not be installed, and many services will be removed from the container. This will result in a faster-booting, but less upgrade-able container.

4.3.1.3. Ubuntu-cloud template

The ubuntu-cloud template creates Ubuntu containers by downloading and extracting the published Ubuntu cloud images. It accepts some of the same options as the ubuntu template, namely *-r release*, *-S sshkey.pub*, *-a arch*, and *-F* to flush the cached image. It also accepts a few extra options. The *-C* option will create a *cloud* container, configured for use with a metadata service. The *-u* option accepts a cloud-init user-data file to configure the container on start. If *-L* is passed, then no locales will be installed. The *-T* option can be used to choose a tarball location to extract in place of the published cloud image tarball. Finally the *-i* option sets a host id for cloud-init, which by default is set to a random string.

4.3.1.4. Other templates

The ubuntu and ubuntu-cloud templates are well supported. Other templates are available however. The debian template creates a Debian based container, using debootstrap much as the ubuntu template does. By default it installs a *debian squeeze* image. An alternate release can be chosen by setting the SUITE environment variable, i.e.:

```
sudo SUITE=sid lxc-create -t debian -n d1
```

Since debian cannot be safely booted inside a container, debian containers will be trimmed as with the *--trim* option to the ubuntu template.

To purge the container image cache, call the template directly and pass it the *--clean* option.

```
sudo SUITE=sid /usr/lib/lxc/templates/lxc-debian --clean
```

A fedora template exists, which creates containers based on fedora releases <= 14. Fedora release 15 and higher are based on systemd, which the template is not yet able to convert into a container-bootable setup. Before the fedora template is able to run, you'll need to make sure that **yum** and **curl** are installed. A fedora 12 container can be created with

```
sudo lxc-create -t fedora -n fedora12 -- -R 12
```

A OpenSuSE template exists, but it requires the **zypper** program, which is not yet packaged. The OpenSuSE template is therefore not supported.

Two more templates exist mainly for experimental purposes. The busybox template creates a very small system container based entirely on busybox. The sshd template creates an application container running sshd in a private network namespace. The host's library and binary directories are bind-mounted into the container, though not its `/home` or `/root`. To create, start, and ssh into an ssh container, you might:

```
sudo lxc-create -t sshd -n ssh1
ssh-keygen -f id
sudo mkdir /var/lib/lxc/ssh1/rootfs/root/.ssh
sudo cp id.pub /var/lib/lxc/ssh1/rootfs/root/.ssh/authorized_keys
sudo lxc-start -n ssh1 -d
ssh -i id root@ssh1.
```

4.3.1.5. Backing Stores

By default, **lxc-create** places the container's root filesystem as a directory tree at `/var/lib/lxc/CN/rootfs.` Another option is to use LVM logical volumes. If a volume group named *lxc* exists, you can create an lvm-backed container called CN using:

```
sudo lxc-create -t ubuntu -n CN -B lvm
```

If you want to use a volume group named schroots, with a 5G xfs filesystem, then you would use

```
sudo lxc-create -t ubuntu -n CN -B lvm --vgname schroots --fssize 5G --fstype xfs
```

4.3.2. Cloning

For rapid provisioning, you may wish to customize a canonical container according to your needs and then make multiple copies of it. This can be done with the **lxc-clone** program. Given an existing container called C1, a new container called C2 can be created using

```
sudo lxc-clone -o C1 -n C2
```

If `/var/lib/lxc` is a btrfs filesystem, then **lxc-clone** will create C2's filesystem as a snapshot of C1's. If the container's root filesystem is lvm backed, then you can specify the *-s* option to create the new rootfs as a lvm snapshot of the original as follows:

```
sudo lxc-clone -s -o C1 -n C2
```

Both lvm and btrfs snapshots will provide fast cloning with very small initial disk usage.

4.3.3. Starting and stopping

To start a container, use **lxc-start -n CN**. By default **lxc-start** will execute `/sbin/init` in the container. You can provide a different program to execute, plus arguments, as further arguments to **lxc-start**:

```
sudo lxc-start -n container /sbin/init loglevel=debug
```

If you do not specify the *-d* (daemon) option, then you will see a console (on the container's `/dev/console`, see *Sezione 4.3.6, «Consoles» [342]* for more information) on the terminal. If you specify the *-d* option, you will not see that console, and lxc-start will immediately exit success - even if a later part of container startup has failed. You can use **lxc-wait** or **lxc-monitor** (see *Sezione 4.3.5, «Monitoring container status » [342]*) to check on the success or failure of the container startup.

To obtain LXC debugging information, use *-o filename -l debuglevel*, for instance:

```
sudo lxc-start -o lxc.debug -l DEBUG -n container
```

Finally, you can specify configuration parameters inline using *-s*. However, it is generally recommended to place them in the container's configuration file instead. Likewise, an entirely alternate config file can be specified with the *-f* option, but this is not generally recommended.

While **lxc-start** runs the container's `/sbin/init`, **lxc-execute** uses a minimal init program called **lxc-init**, which attempts to mount `/proc`, `/dev/mqueue`, and `/dev/shm`, executes the programs specified on the command line, and waits for those to finish executing. **lxc-start** is intended to be used for *system containers*, while **lxc-execute** is intended for *application containers* (see *this article*[23] for more).

You can stop a container several ways. You can use **shutdown**, **poweroff** and **reboot** while logged into the container. To cleanly shut down a container externally (i.e. from the host), you can issue

[23] https://www.ibm.com/developerworks/linux/library/l-lxc-containers/

the **sudo lxc-shutdown -n CN** command. This takes an optional timeout value. If not specified, the command issues a SIGPWR signal to the container and immediately returns. If the option is used, as in **sudo lxc-shutdown -n CN -t 10**, then the command will wait the specified number of seconds for the container to cleanly shut down. Then, if the container is still running, it will kill it (and any running applications). You can also immediately kill the container (without any chance for applications to cleanly shut down) using **sudo lxc-stop -n CN**. Finally, **lxc-kill** can be used more generally to send any signal number to the container's init.

While the container is shutting down, you can expect to see some (harmless) error messages, as follows:

```
$ sudo poweroff
[sudo] password for ubuntu: =

$ =

Broadcast message from ubuntu@cn1
        (/dev/lxc/console) at 18:17 ...

The system is going down for power off NOW!
 * Asking all remaining processes to terminate...
   ...done.
 * All processes ended within 1 seconds....
   ...done.
 * Deconfiguring network interfaces...
   ...done.
 * Deactivating swap...
   ...fail!
umount: /run/lock: not mounted
umount: /dev/shm: not mounted
mount: / is busy
 * Will now halt
```

A container can be frozen with **sudo lxc-freeze -n CN**. This will block all its processes until the container is later unfrozen using **sudo lxc-unfreeze -n CN**.

4.3.4. Lifecycle management hooks

Beginning with Ubuntu 12.10, it is possible to define hooks to be executed at specific points in a container's lifetime:

- Pre-start hooks are run in the host's namespace before the container ttys, consoles, or mounts are up. If any mounts are done in this hook, they should be cleaned up in the post-stop hook.
- Pre-mount hooks are run in the container's namespaces, but before the root filesystem has been mounted. Mounts done in this hook will be automatically cleaned up when the container shuts down.
- Mount hooks are run after the container filesystems have been mounted, but before the container has called **pivot_root** to change its root filesystem.

- Start hooks are run immediately before executing the container's init. Since these are executed after pivoting into the container's filesystem, the command to be executed must be copied into the container's filesystem.
- Post-stop hooks are executed after the container has been shut down.

If any hook returns an error, the container's run will be aborted. Any *post-stop* hook will still be executed. Any output generated by the script will be logged at the debug priority.

See *Sezione 4.4.5, «Other configuration options» [348]* for the configuration file format with which to specify hooks. Some sample hooks are shipped with the lxc package to serve as an example of how to write and use such hooks.

4.3.5. Monitoring container status

Two commands are available to monitor container state changes. **lxc-monitor** monitors one or more containers for any state changes. It takes a container name as usual with the *-n* option, but in this case the container name can be a posix regular expression to allow monitoring desirable sets of containers. **lxc-monitor** continues running as it prints container changes. **lxc-wait** waits for a specific state change and then exits. For instance,

```
sudo lxc-monitor -n cont[0-5]*
```

would print all state changes to any containers matching the listed regular expression, whereas

```
sudo lxc-wait -n cont1 -s 'STOPPED|FROZEN'
```

will wait until container cont1 enters state STOPPED or state FROZEN and then exit.

4.3.6. Consoles

Containers have a configurable number of consoles. One always exists on the container's `/dev/console`. This is shown on the terminal from which you ran **lxc-start**, unless the *-d* option is specified. The output on `/dev/console` can be redirected to a file using the *-c console-file* option to **lxc-start**. The number of extra consoles is specified by the **lxc.tty** variable, and is usually set to 4. Those consoles are shown on `/dev/ttyN` (for 1 <= N <= 4). To log into console 3 from the host, use

```
sudo lxc-console -n container -t 3
```

or if the *-t N* option is not specified, an unused console will be automatically chosen. To exit the console, use the escape sequence Ctrl-a q. Note that the escape sequence does not work in the console resulting from **lxc-start** without the *-d* option.

Each container console is actually a Unix98 pty in the host's (not the guest's) pty mount, bind-mounted over the guest's `/dev/ttyN` and `/dev/console`. Therefore, if the guest unmounts those or otherwise tries to access the actual character device **4:N**, it will not be serving getty to the LXC consoles. (With the default settings, the container will not be able to access that character device and getty will therefore fail.) This can easily happen when a boot script blindly mounts a new `/dev`.

4.3.7. Container Inspection

Several commands are available to gather information on existing containers. **lxc-ls** will report all existing containers in its first line of output, and all running containers in the second line. **lxc-list** provides the same information in a more verbose format, listing running containers first and stopped containers next. **lxc-ps** will provide lists of processes in containers. To provide **ps** arguments to **lxc-ps**, prepend them with --. For instance, for listing of all processes in container plain,

```
sudo lxc-ps -n plain -- -ef
```

lxc-info provides the state of a container and the pid of its init process. **lxc-cgroup** can be used to query or set the values of a container's control group limits and information. This can be more convenient than interacting with the **cgroup** filesystem. For instance, to query the list of devices which a running container is allowed to access, you could use

```
sudo lxc-cgroup -n CN devices.list
```

or to add mknod, read, and write access to `/dev/sda`,

```
sudo lxc-cgroup -n CN devices.allow "b 8:* rwm"
```

and, to limit it to 300M of RAM,

```
lxc-cgroup -n CN memory.limit_in_bytes 300000000
```

lxc-netstat executes **netstat** in the running container, giving you a glimpse of its network state.

lxc-backup will create backups of the root filesystems of all existing containers (except lvm-based ones), using **rsync** to back the contents up under `/var/lib/lxc/CN/rootfs.backup.1`. These backups can be restored using **lxc-restore.** However, **lxc-backup** and **lxc-restore** are fragile with respect to customizations and therefore their use is not recommended.

4.3.8. Destroying containers

Use **lxc-destroy** to destroy an existing container.

```
sudo lxc-destroy -n CN
```

If the container is running, **lxc-destroy** will exit with a message informing you that you can force stopping and destroying the container with

```
sudo lxc-destroy -n CN -f
```

4.3.9. Advanced namespace usage

One of the Linux kernel features used by LXC to create containers is private namespaces. Namespaces allow a set of tasks to have private mappings of names to resources for things like pathnames and process IDs. (See *Sezione 4.10, «Risorse» [353]* for a link to more information). Unlike control groups and other mount features which are also used to create containers, namespaces cannot be manipulated using a filesystem interface. Therefore, LXC ships with the **lxc-unshare** program, which is mainly for testing. It provides the ability to create new tasks in private namespaces. For instance,

```
sudo lxc-unshare -s 'MOUNT|PID' /bin/bash
```

creates a bash shell with private pid and mount namespaces. In this shell, you can do

```
root@ubuntu:~# mount -t proc proc /proc
root@ubuntu:~# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  6 10:20 pts/9    00:00:00 /bin/bash
root       110     1  0 10:20 pts/9    00:00:00 ps -ef
```

so that **ps** shows only the tasks in your new namespace.

4.3.10. Ephemeral containers

Ephemeral containers are one-time containers. Given an existing container CN, you can run a command in an ephemeral container created based on CN, with the host's jdoe user bound into the container, using:

```
lxc-start-ephemeral -b jdoe -o CN -- /home/jdoe/run_my_job
```

When the job is finished, the container will be discarded.

4.3.11. Container Commands

Following is a table of all container commands:

Tabella 20.1. Container commands

Command	Synopsis
lxc-attach	(NOT SUPPORTED) Run a command in a running container
lxc-backup	Back up the root filesystems for all lvm-backed containers
lxc-cgroup	View and set container control group settings
lxc-checkconfig	Verify host support for containers
lxc-checkpoint	(NOT SUPPORTED) Checkpoint a running container
lxc-clone	Clone a new container from an existing one
lxc-console	Open a console in a running container
lxc-create	Create a new container
lxc-destroy	Destroy an existing container
lxc-execute	Run a command in a (not running) application container
lxc-freeze	Freeze a running container
lxc-info	Print information on the state of a container
lxc-kill	Send a signal to a container's init
lxc-list	List all containers
lxc-ls	List all containers with shorter output than lxc-list
lxc-monitor	Monitor state changes of one or more containers
lxc-netstat	Execute netstat in a running container
lxc-ps	View process info in a running container
lxc-restart	(NOT SUPPORTED) Restart a checkpointed container
lxc-restore	Restore containers from backups made by lxc-backup
lxc-setcap	(NOT RECOMMENDED) Set file capabilities on LXC tools
lxc-setuid	(NOT RECOMMENDED) Set or remove setuid bits on LXC tools
lxc-shutdown	Safely shut down a container
lxc-start	Start a stopped container
lxc-start-ephemeral	Start an ephemeral (one-time) container

Command	Synopsis
lxc-stop	Immediately stop a running container
lxc-unfreeze	Unfreeze a frozen container
lxc-unshare	Testing tool to manually unshare namespaces
lxc-version	Print the version of the LXC tools
lxc-wait	Wait for a container to reach a particular state

4.4. Configuration File

LXC containers are very flexible. The Ubuntu lxc package sets defaults to make creation of Ubuntu system containers as simple as possible. If you need more flexibility, this chapter will show how to fine-tune your containers as you need.

Detailed information is available in the **lxc.conf(5)** man page. Note that the default configurations created by the ubuntu templates are reasonable for a system container and usually do not need customization.

4.4.1. Choosing configuration files and options

The container setup is controlled by the LXC configuration options. Options can be specified at several points:

- During container creation, a configuration file can be specified. However, creation templates often insert their own configuration options, so we usually specify only network configuration options at this point. For other configuration, it is usually better to edit the configuration file after container creation.
- The file `/var/lib/lxc/CN/config` is used at container startup by default.
- **lxc-start** accepts an alternate configuration file with the *-f filename* option.
- Specific configuration variables can be overridden at **lxc-start** using **-***s key=value*. It is generally better to edit the container configuration file.

4.4.2. Configurare la rete

Container networking in LXC is very flexible. It is triggered by the **lxc.network.type** configuration file entries. If no such entries exist, then the container will share the host's networking stack. Services and connections started in the container will be using the host's IP address. If at least one **lxc.network.type** entry is present, then the container will have a private (layer 2) network stack. It will have its own network interfaces and firewall rules. There are several options for **lxc.network.type**:

- **lxc.network.type=empty**: The container will have no network interfaces other than loopback.
- **lxc.network.type=veth**: This is the default when using the ubuntu or ubuntu-cloud templates, and creates a veth network tunnel. One end of this tunnel becomes the network interface inside the

container. The other end is attached to a bridged on the host. Any number of such tunnels can be created by adding more **lxc.network.type=veth** entries in the container configuration file. The bridge to which the host end of the tunnel will be attached is specified with **lxc.network.link = lxcbr0**.

- **lxc.network.type=phys** A physical network interface (i.e. eth2) is passed into the container.

Two other options are to use vlan or macvlan, however their use is more complicated and is not described here. A few other networking options exist:

- **lxc.network.flags** can only be set to *up* and ensures that the network interface is up.
- **lxc.network.hwaddr** specifies a mac address to assign the the nic inside the container.
- **lxc.network.ipv4** and **lxc.network.ipv6** set the respective IP addresses, if those should be static.
- **lxc.network.name** specifies a name to assign inside the container. If this is not specified, a good default (i.e. eth0 for the first nic) is chosen.
- **lxc.network.lxcscript.up** specifies a script to be called after the host side of the networking has been set up. See the **lxc.conf(5)** manual page for details.

4.4.3. Control group configuration

Cgroup options can be specified using **lxc.cgroup** entries. **lxc.cgroup.subsystem.item = value** instructs LXC to set cgroup **subsystem**'s **item** to **value**. It is perhaps simpler to realize that this will simply write **value** to the file **item** for the container's control group for subsystem **subsystem**. For instance, to set the memory limit to 320M, you could add

```
lxc.cgroup.memory.limit_in_bytes = 320000000
```

which will cause 320000000 to be written to the file `/sys/fs/cgroup/memory/lxc/CN/limit_in_bytes`.

4.4.4. Rootfs, mounts and fstab

An important part of container setup is the mounting of various filesystems into place. The following is an example configuration file excerpt demonstrating the commonly used configuration options:

```
lxc.rootfs = /var/lib/lxc/CN/rootfs
lxc.mount.entry=proc /var/lib/lxc/CN/rootfs/proc proc nodev,noexec,nosuid 0 0
lxc.mount = /var/lib/lxc/CN/fstab
```

The first line says that the container's root filesystem is already mounted at `/var/lib/lxc/CN/rootfs`. If the filesystem is a block device (such as an LVM logical volume), then the path to the block device must be given instead.

Each **lxc.mount.entry** line should contain an item to mount in valid fstab format. The target directory should be prefixed by `/var/lib/lxc/CN/rootfs`, even if **lxc.rootfs** points to a block device.

Finally, **lxc.mount** points to a file, in fstab format, containing further items to mount. Note that all of these entries will be mounted by the host before the container init is started. In this way it is possible to bind mount various directories from the host into the container.

4.4.5. Other configuration options

- **lxc.cap.drop** can be used to prevent the container from having or ever obtaining the listed capabilities. For instance, including

  ```
  lxc.cap.drop = sys_admin
  ```

  will prevent the container from mounting filesystems, as well as all other actions which require cap_sys_admin. See the **capabilities(7)** manual page for a list of capabilities and their meanings.
- **lxc.aa_profile = lxc-CN-profile** specifies a custom Apparmor profile in which to start the container. See *Sezione 4.2.6, «Apparmor» [334]* for more information.
- **lxc.console=/path/to/consolefile** will cause console messages to be written to the specified file.
- **lxc.arch** specifies the architecture for the container, for instance x86, or x86_64.
- **lxc.tty=5** specifies that 5 consoles (in addition to `/dev/console`) should be created. That is, consoles will be available on `/dev/tty1` through `/dev/tty5`. The ubuntu templates set this value to 4.
- **lxc.pts=1024** specifies that the container should have a private (Unix98) devpts filesystem mount. If this is not specified, then the container will share `/dev/pts` with the host, which is rarely desired. The number 1024 means that 1024 ptys should be allowed in the container, however this number is currently ignored. Before starting the container init, LXC will do (essentially) a

  ```
  sudo mount -t devpts -o newinstance devpts /dev/pts
  ```

  inside the container. It is important to realize that the container should not mount devpts filesystems of its own. It may safely do bind or move mounts of its mounted `/dev/pts`. But if it does

  ```
  sudo mount -t devpts devpts /dev/pts
  ```

  it will remount the host's devpts instance. If it adds the newinstance mount option, then it will mount a new private (empty) instance. In neither case will it remount the instance which was set up by LXC. For this reason, and to prevent the container from using the host's ptys, the default

Apparmor policy will not allow containers to mount devpts filesystems after the container's init has been started.

- **lxc.devttydir** specifies a directory under `/dev` in which LXC will create its console devices. If this option is not specified, then the ptys will be bind-mounted over `/dev/console` and `/dev/ttyN`. However, rare package updates may try to blindly *rm -f* and then *mknod* those devices. They will fail (because the file has been bind-mounted), causing the package update to fail. When **lxc.devttydir** is set to LXC, for instance, then LXC will bind-mount the console ptys onto `/dev/lxc/console` and `/dev/lxc/ttyN`, and subsequently symbolically link them to `/dev/console` and `/dev/ttyN`. This allows the package updates to succeed, at the risk of making future gettys on those consoles fail until the next reboot. This problem will be ideally solved with device namespaces.
- The **lxc.hook.** options specify programs to run at various points in a container's life cycle. See *Sezione 4.3.4, «Lifecycle management hooks» [341]* for more information on these hooks. To have multiple hooks called at any point, list them in multiple entries. The possible values, whose precise meanings are described in *Sezione 4.3.4, «Lifecycle management hooks» [341]*, are
  - **lxc.hook.pre-start**
  - **lxc.hook.pre-mount**
  - **lxc.hook.mount**
  - **lxc.hook.start**
  - **lxc.hook.post-stop**
- The **lxc.include** option specifies another configuration file to be loaded. This allows common configuration sections to be defined once and included by several containers, simplifying updates of the common section.
- The **lxc.seccomp** option (introduced with Ubuntu 12.10) specifies a file containing a *seccomp* policy to load. See *Sezione 4.9, «Sicurezza» [352]* for more information on seccomp in lxc.

4.5. Updates in Ubuntu containers

Because of some limitations which are placed on containers, package upgrades at times can fail. For instance, a package install or upgrade might fail if it is not allowed to create or open a block device. This often blocks all future upgrades until the issue is resolved. In some cases, you can work around this by chrooting into the container, to avoid the container restrictions, and completing the upgrade in the chroot.

Some of the specific things known to occasionally impede package upgrades include:

- The container modifications performed when creating containers with the --trim option.
- Actions performed by lxcguest. For instance, because `/lib/init/fstab` is bind-mounted from another file, mountall upgrades which insist on replacing that file can fail.
- The over-mounting of console devices with ptys from the host can cause trouble with udev upgrades.

- Apparmor policy and devices cgroup restrictions can prevent package upgrades from performing certain actions.
- Capabilities dropped by use of **lxc.cap.drop** can likewise stop package upgrades from performing certain actions.

4.6. Libvirt LXC

Libvirt is a powerful hypervisor management solution with which you can administer Qemu, Xen and LXC virtual machines, both locally and remote. The libvirt LXC driver is a separate implementation from what we normally call *LXC*. A few differences include:

- Configuration is stored in xml format
- There no tools to facilitate container creation
- By default there is no console on `/dev/console`
- There is no support (yet) for container reboot or full shutdown

4.6.1. Converting a LXC container to libvirt-lxc

Sezione 4.3.1, «Creating Containers» [336] showed how to create LXC containers. If you've created a valid LXC container in this way, you can manage it with libvirt. Fetch a sample xml file from

```
wget http://people.canonical.com/~serge/o1.xml
```

Edit this file to replace the container name and root filesystem locations. Then you can define the container with:

```
virsh -c lxc:/// define o1.xml
```

4.6.2. Creating a container from cloud image

If you prefer to create a pristine new container just for LXC, you can download an ubuntu cloud image, extract it, and point a libvirt LXC xml file to it. For instance, find the url for a root tarball for the latest daily Ubuntu 12.04 LTS cloud image using

```
url1=`ubuntu-cloudimg-query precise daily $arch --format "%{url}\n"`
url=`echo $url1 | sed -e 's/.tar.gz/-root\0/'`
wget $url
filename=`basename $url`
```

Extract the downloaded tarball, for instance

```
mkdir $HOME/c1
cd $HOME/c1
sudo tar zxf $filename
```

Download the xml template

```
wget http://people.canonical.com/~serge/o1.xml
```

In the xml template, replace the name o1 with c1 and the source directory `/var/lib/lxc/o1/rootfs` with `$HOME/c1`. Then define the container using

```
virsh define o1.xml
```

4.6.3. Interacting with libvirt containers

As we've seen, you can create a libvirt-lxc container using

```
virsh -c lxc:/// define container.xml
```

To start a container called *container*, use

```
virsh -c lxc:/// start container
```

To stop a running container, use

```
virsh -c lxc:/// destroy container
```

Note that whereas the **lxc-destroy** command deletes the container, the **virsh destroy** command stops a running container. To delete the container definition, use

```
virsh -c lxc:/// undefine container
```

To get a console to a running container, use

```
virsh -c lxc:/// console container
```

Exit the console by simultaneously pressing control and].

4.7. The lxcguest package

In the 11.04 (Natty) and 11.10 (Oneiric) releases of Ubuntu, a package was introduced called *lxcguest*. An unmodified root image could not be safely booted inside a container, but an image with the lxcguest package installed could be booted as a container, on bare hardware, or in a Xen, kvm, or VMware virtual machine.

As of the 12.04 LTS release, the work previously done by the lxcguest package was pushed into the core packages, and the lxcguest package was removed. As a result, an unmodified 12.04 LTS image can be booted as a container, on bare hardware, or in a Xen, kvm, or VMware virtual machine. To use an older release, the lxcguest package should still be used.

4.8. Python api

As of 12.10 (Quantal) a python3-lxc package is available which provides a python module, called **lxc**, for managing lxc containers. An example python session to create and start an Ubuntu container called `C1`, then wait until it has been shut down, would look like:

```
# sudo python3
Python 3.2.3 (default, Aug 28 2012, 08:26:03)
[GCC 4.7.1 20120814 (prerelease)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import lxc
__main__:1: Warning: The python-lxc API isn't yet stable and may change at any p
oint in the future.
>>> c=lxc.Container("C1")
>>> c.create("ubuntu")
True
>>> c.start()
True
>>> c.wait("STOPPED")
True
```

Debug information for containers started with the python API will be placed in `/var/log/lxccontainer.log`.

4.9. Sicurezza

A namespace maps ids to resources. By not providing a container any id with which to reference a resource, the resource can be protected. This is the basis of some of the security afforded to container

users. For instance, IPC namespaces are completely isolated. Other namespaces, however, have various *leaks* which allow privilege to be inappropriately exerted from a container into another container or to the host.

By default, LXC containers are started under a Apparmor policy to restrict some actions. However, while stronger security is a goal for future releases, in 12.04 LTS the goal of the Apparmor policy is not to stop malicious actions but rather to stop accidental harm of the host by the guest. The details of AppArmor integration with lxc are in section *Sezione 4.2.6, «Apparmor» [334]*

4.9.1. Exploitable system calls

It is a core container feature that containers share a kernel with the host. Therefore if the kernel contains any exploitable system calls the container can exploit these as well. Once the container controls the kernel it can fully control any resource known to the host.

Since Ubuntu 12.10 (Quantal) a container can also be constrained by a seccomp filter. Seccomp is a new kernel feature which filters the system calls which may be used by a task and its children. While improved and simplified policy management is expected in the near future, the current policy consists of a simple whitelist of system call numbers. The policy file begins with a version number (which must be 1) on the first line and a policy type (which must be 'whitelist') on the second line. It is followed by a list of numbers, one per line.

In general to run a full distribution container a large number of system calls will be needed. However for application containers it may be possible to reduce the number of available system calls to only a few. Even for system containers running a full distribution security gains may be had, for instance by removing the 32-bit compatibility system calls in a 64-bit container. See *Sezione 4.4.5, «Other configuration options» [348]* for details of how to configure a container to use seccomp. By default, no seccomp policy is loaded.

4.10. Risorse

- The DeveloperWorks article *LXC: Linux container tools*[24] was an early introduction to the use of containers.
- The *Secure Containers Cookbook*[25] demonstrated the use of security modules to make containers more secure.
- Manual pages referenced above can be found at:

  capabilities[26]
  lxc.conf[27]

- The upstream LXC project is hosted at *Sourceforge*[28].

24 https://www.ibm.com/developerworks/linux/library/l-lxc-containers/
25 http://www.ibm.com/developerworks/linux/library/l-lxc-security/index.html
26 http://manpages.ubuntu.com/manpages/en/man7/capabilities.7.html
27 http://manpages.ubuntu.com/manpages/en/man5/lxc.conf.5.html
28 http://lxc.sf.net

- LXC security issues are listed and discussed at *the LXC Security wiki page*[29]
- For more on namespaces in Linux, see: S. Bhattiprolu, E. W. Biederman, S. E. Hallyn, and D. Lezcano. Virtual Servers and Check- point/Restart in Mainstream Linux. SIGOPS Op- erating Systems Review, 42(5), 2008.

[29] http://wiki.ubuntu.com/LxcSecurity

Capitolo 21. Cluster

1. DRBD

DRDB (Distributed Replicated Block Device) replica i device a blocchi tra diversi host. La replica è trasparente alle applicazioni sul sistema host e qualsiasi device a blocchi (disco fisso, partizione, RAID, volume logico) può essere replicato.

Per utilizzare drbd, per prima cosa è necessario installare i pacchetti necessari. In un terminale digitare:

```
sudo apt-get install drbd8-utils
```

Se si sta usando il *kernel virtuale* come parte di una macchina virtuale, è necessario compilare il modulo drbd. Potrebbe anche essere più semplice installare il pacchetto linux-server nella macchina virtuale.

In questa sezione viene indicato come configurare drbd per replicare tra due host una partizione `/srv` separata con file system ext3. La dimensione della partizione non è rilevante, ma entrambe le partizioni devono avere la stessa dimensione.

1.1. Configurazione

I due host in questo esempio sono chiamati *drbd01* e *drbd02* ed è necessario configurarne la risoluzione del nome attraverso DNS o con il file `/etc/hosts`. Per maggiori informazioni, consultare *Capitolo 8, DNS (Domain Name Service) [140]*.

- Per configurare drbd, sul primo host modificare il file `/etc/drbd.conf`:

```
global { usage-count no; }
common { syncer { rate 100M; } }
resource r0 {
        protocol C;
        startup {
                wfc-timeout  15;
                degr-wfc-timeout 60;
        }
        net {
                cram-hmac-alg sha1;
                shared-secret "secret";
        }
        on drbd01 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.1:7788;
                meta-disk internal;
        }
        on drbd02 {
                device /dev/drbd0;
                disk /dev/sdb1;
```

```
                address 192.168.0.2:7788;
                meta-disk internal;
        }
}
```

All'interno del file /etc/drbd.conf sono disponibili molte opzioni, ma per questo esempio i valori predefinito sono sufficienti.

- Copiare il file /etc/drbd.conf sul secondo host:

```
scp /etc/drbd.conf drbd02:~
```

- Sull'host *drbd02*, spostare il file in /etc:

```
sudo mv drbd.conf /etc/
```

- Utilizzando l'utilità drbdadm, inizializzare l'archivio dei meta-dati. Su ogni singolo server eseguire il seguente comando:

```
sudo drbdadm create-md r0
```

- Su entrambi gli host, avviare il demone drbd:

```
sudo service drbd start
```

- Sull'host *drbd01*, o su qualsiasi host primario configurato, digitare:

```
sudo drbdadm -- --overwrite-data-of-peer primary all
```

- Una volta eseguito il comando precedente, inizierà la sincronizzazione dei dati con l'host secondario. Per visualizzare l'avanzamento, su *drbd02*, digitare il seguente comando:

```
watch -n1 cat /proc/drbd
```

  Per fermare l'operazione di controllo, premere *Ctrl+c*.

- Infine, aggiungere un file system a /dev/drbd0 e montarlo:

```
sudo mkfs.ext3 /dev/drbd0
sudo mount /dev/drbd0 /srv
```

1.2. Test

Per verificare che i dati siano effettivamente sincronizzati tra gli host, copiare alcuni file sull'host primario, *drbd01*, nella directory /srv:

```
sudo cp -r /etc/default /srv
```

Smontare /srv:

```
sudo umount /srv
```

Retrocedere il server *primario* a ruolo di *secondario*:

```
sudo drbdadm secondary r0
```

Ora, *promuovere* il server *secondario* a *primario*:

```
sudo drbdadm primary r0
```

Per completare, montare la partizione:

```
sudo mount /dev/drbd0 /srv
```

Usando *ls* dovrebbe essere possibile vedere il file `/srv/default` copiato dal precedente host *primario drbd01*.

1.3. Riferimenti

- Per maggiori informazioni riguardo DRBD, consultare il *sito web di DRBD*[1].
- The *drbd.conf man page*[2] contains details on the options not covered in this guide.
- Also, see the *drbdadm man page*[3].
- Ulteriori informazioni sono disponibili nella *documentazione online*[4].

[1] http://www.drbd.org/
[2] http://manpages.ubuntu.com/manpages/quantal/en/man5/drbd.conf.5.html
[3] http://manpages.ubuntu.com/manpages/quantal/en/man8/drbdadm.8.html
[4] https://help.ubuntu.com/community/DRBD

Capitolo 22. VPN

OpenVPN è una soluzione per Virtual Private Networking (VPN) fornita dai repository Ubuntu: è versatile, affidabile e sicuro; appartiene alla famiglia degli stack SSL/TLS VPN (diversa dalle VPN di tipo IPSec). Questo capitolo illustra l'installazione e la configurazione di OpenVPN per creare una VPN.

1. OpenVPN

Nel caso in cui si richieda qualcosa in più delle chiavi pre-condivise, OpenVPN offre una facile configurazione e utilizza una infrastruttura a chiave pubblica (Public Key Infrastructure, PKI) grazie a certificati SSL/TLS per l'autenticazione e lo scambio di chiavi tra server e client della VPN. OpenVPN si può utilizzare in modalità router o bridge e ed è configurabile per l'uso di UDP o TCP. Può essere configurato anche il numero di porta, ma quella ufficiale utilizzata per tutte le comunicazioni è la 1194. Le implementazioni client di VPN sono disponibili praticamente per qualunque SO, incluse tutte le distribuzioni Linux, OS X, Windows e i router WLAN basati su OpenWRT.

1.1. Installazione del server

Per installare openvpn, in un terminale, digitare:

```
sudo apt-get install openvpn
```

1.2. Configurazione della Infrastruttura a chiave pubblica

Il primo passo nella configurazione di OpenVPN è stabilire una PKI (Public Key Infrastructure), che consiste di:

- un certificato separato (noto come chiave pubblica) e una chiave privata per il server e ogni client, e
- un certificato master ottenuto da una Autorità di Certificazione (CA) e relativa chiave, utilizzati per firmare i certificati del server e dei client.

OpenVPN supporta l'autenticazione bidirezionale basata su certificati e questo significa che il client deve autenticare il certificato del server e il server deve autenticare il certificato del client, prima che sia stabilita una relazione di fiducia reciproca.

Sia il server che il client si autenticheranno reciprocamente prima controllando che il certificato presentato sia firmato dall'autorità di certificazione (CA) e quindi verificando le informazioni contenute nell'intestazione del certificato appena autenticato, quali il nome comune o il tipo di certificato (client o server).

1.2.1. Impostazione dell'Autorità di Certificazione

Per impostare la propria Autorità di Certificazione (CA) e generare certificati e chiavi per un server e più client OpenVPN, per prima cosa copiare la directory `easy-rsa` in `/etc/openvpn`. Questo assicura di non perdere tutte le modifiche agli script quando il pacchetto verrà aggiornato: in un terminale, diventare utente root e:

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

Modificare quindi il file `/etc/openvpn/easy-rsa/vars` adattando al proprio ambiente quanto segue:

```
export KEY_COUNTRY="IT"
export KEY_PROVINCE="Roma"
export KEY_CITY="Roma"
export KEY_ORG="Società di esempio"
export KEY_EMAIL="mario@example.com"
```

Digitare il seguente comando per generare il certificato master dell'Autorità di Certificazione (CA) e la chiave:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-ca
```

1.2.2. Certificati server

Successivamente, verrà generato un certificato e una chiave privata per il server:

```
./build-key-server myservername
```

Come nel passo precedente, molti parametri possono essere lasciati come predefiniti. Due altre domande richiedono risposte positive, «Sign the certificate? [y/n]» e «1 out of 1 certificate requests certified, commit? [y/n]».

È necessario generare i parametri Diffie-Hellman per il server OpenVPN:

```
./build-dh
```

Tutti i certificati e le chiavi sono stati generati nella sotto-directory keys/: la comune procedura prevede che siano copiati in /etc/openvpn/:

```
cd keys/
cp myservername.crt myservername.key ca.crt dh1024.pem /etc/openvpn/
```

1.2.3. Certificati client

Il client VPN necessita anche di un certificato per autenticarsi sul server: di solito viene creato un diverso certificato per ogni client. Per creare il certificato, come utente root digitare quanto segue in un terminale:

```
cd /etc/openvpn/easy-rsa/
source vars
./build-key client1
```

Copiare i seguenti file nel client, utilizzando un metodo sicuro:

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/client1.crt
- /etc/openvpn/easy-rsa/keys/client1.key

Dato che i certificati client e le chiavi sono richieste solo sul client, è opportuno rimuoverli dal server.

1.3. Semplice configurazione del server

Con l'installazione di OpenVPN si sono ottenuti questi file di configurazione d'esempio (e molti di più, se si controlla):

```
root@server:/# ls -l /usr/share/doc/openvpn/examples/sample-config-files/
total 68
-rw-r--r-- 1 root root 3427 2011-07-04 15:09 client.conf
-rw-r--r-- 1 root root 4141 2011-07-04 15:09 server.conf.gz
```

Per prima cosa copiare e decomprimere unpacking server.conf.gz in /etc/openvpn/server.conf.

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
```

Modificare `/etc/openvpn/server.conf` per assicurarsi che le seguenti righe puntino ai certificati e alle chiavi create come spiegato nella sezione precedente.

```
ca ca.crt
cert myservername.crt
key myservername.key
dh dh1024.pem
```

Questa è la minima configurazione necessaria per ottenere un server OpenVPN funzionante: è possibile usare tutte le impostazioni predefinite del file d'esempio server.conf. Ora avviare il server: i messaggi di accesso e di errore sono nel syslog.

```
root@server:/etc/openvpn# service openvpn start
 * Starting virtual private network daemon(s)...
   *   Autostarting VPN 'server'                     [ OK ]
```

Ora controllare se OpenVPN ha creato un'interfaccia tun0

```
root@server:/etc/openvpn# ifconfig tun0
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1 P-t-P:10.8.0.2 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
[...]
```

1.4. Semplice configurazione del client

Ci sono diverse implementazioni OpenVPN per client, con e senza GUI: maggiori informazioni sui client verranno fornite in una successiva sezione. Per il momento verrà utilizzato OpenVPN client per Ubuntu, che è lo stesso eseguibile usato per il server. È pertanto necessario installare nuovamente il pacchetto openvpn sul client:

```
sudo apt-get install openvpn
```

Questa volta copiare il file di configurazione d'esempio client.conf in /etc/openvpn/.

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/
```

Copiare le chiavi client e il certificato della CA, creati come indicato in una precedente sezione, per esempio in /etc/openvpn/ e modificare `/etc/openvpn/client.conf` per assicurarsi che le righe seguenti puntino a quei file; se i file sono in /etc/openvpn/ si può omettere il percorso.

```
ca ca.crt
cert client1.crt
key client1.key
```

È necessario almeno specificare il nome o l'indirizzo del server Open VPN; assicurarsi che la parola chiave «client» sia nella configurazione: è questo che abilita la modalità client.

```
client
remote vpnserver.example.com 1194
```

Ora avviare il client OpenVPN:

```
root@client:/etc/openvpn# service openvpn start
 * Starting virtual private network daemon(s)...
   *   Autostarting VPN 'client'                          [ OK ]
```

Controllare se è stata creata un'interfaccia tun0:

```
root@client:/etc/openvpn# ifconfig tun0
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.6 P-t-P:10.8.0.5 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
```

Controllare se è possibile inviare un ping al server OpenVPN

```
root@client:/etc/openvpn# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_req=1 ttl=64 time=0.920 ms
```

Il server OpenVPN usa sempre il primo indirizzo utilizzabile nella rete client e solo se quell'IP è raggiungibile con un ping; per esempio, se è stata configurata come maschera della rete client una /24, verrà usato l'indirizzo .1. L'indirizzo P-t-P presente nell'output di ifconfig sopra riportato normalmente non risponde alle richieste di ping.

Controllare i propri percorsi:

```
root@client:/etc/openvpn# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
10.8.0.5 0.0.0.0 255.255.255.255 UH 0 0 0 tun0
10.8.0.1 10.8.0.5 255.255.255.255 UGH 0 0 0 tun0
192.168.42.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 192.168.42.1 0.0.0.0 UG 0 0 0 eth0
```

1.5. Prima risoluzione di problemi

Se quanto sopra non funziona, controllare questo:

- Controllare il syslog, per es. grep -i vpn /var/log/syslog
- Il client riesce a connettersi al server? Forse un firewall sta bloccando l'accesso? Controllare il syslog sul server.
- Sia il client che il server devono usare lo stesso protocollo e la medesima porta, per es. UDP porta 1194, controllare le opzioni di configurazione di porta e protocollo
- Client and server must use same config regarding compression, see comp-lzo config option
- Client and server must use same config regarding bridged vs routed mode, see server vs server-bridge config option

1.6. Configurazione avanzata

1.6.1. Advanced routed VPN configuration on server

The above is a very simple working VPN. The client can access services on the VPN server machine through an encrypted tunnel. If you want to reach more servers or anything in other networks, push some routes to the clients. E.g. if your company's network can be summarized to the network 192.168.0.0/16, you could push this route to the clients. But you will also have to change the routing for the way back - your servers need to know a route to the VPN client-network.

Or you might push a default gateway to all the clients to send all their internet traffic to the VPN gateway first and from there via the company firewall into the internet. This section shows you some possible options.

Push routes to the client to allow it to reach other private subnets behind the server. Remember that these private subnets will also need to know to route the OpenVPN client address pool (10.8.0.0/24) back to the OpenVPN server.

```
push "route 10.0.0.0 255.0.0.0"
```

If enabled, this directive will configure all clients to redirect their default network gateway through the VPN, causing all IP traffic such as web browsing and DNS lookups to go through the VPN (the OpenVPN server machine or your central firewall may need to NAT the TUN/TAP interface to the internet in order for this to work properly).

```
push "redirect-gateway def1 bypass-dhcp"
```

Configurare la modalità server e fornire una sottorete VPN per permettere a OpenVPN di trarvi gli indirizzi client. Il server prenderà 10.8.0.1 per sé stesso, il resto sarà reso disponibile ai client, ognuno dei quali sarà in grado di raggiungere il server a 10.8.0.1. Commentare questa riga se si sta effettuando un ponte ethernet.

```
server 10.8.0.0 255.255.255.0
```

Maintain a record of client to virtual IP address associations in this file. If OpenVPN goes down or is restarted, reconnecting clients can be assigned the same virtual IP address from the pool that was previously assigned.

```
ifconfig-pool-persist ipp.txt
```

Inviare i server DNS al client.

```
push "dhcp-option DNS 10.0.0.2"
push "dhcp-option DNS 10.1.0.2"
```

Allow client to client communication.

```
client-to-client
```

Enable compression on the VPN link.

```
comp-lzo
```

The keepalive directive causes ping-like messages to be sent back and forth over the link so that each side knows when the other side has gone down. Ping every 1 second, assume that remote peer is down if no ping received during a 3 second time period.

```
keepalive 1 3
```

It's a good idea to reduce the OpenVPN daemon's privileges after initialization.

```
user nessuno
group nessungruppo
```

OpenVPN 2.0 includes a feature that allows the OpenVPN server to securely obtain a username and password from a connecting client, and to use that information as a basis for authenticating the client. To use this authentication method, first add the auth-user-pass directive to the client configuration. It will direct the OpenVPN client to query the user for a username/password, passing it on to the server over the secure TLS channel.

```
# client config!
auth-user-pass
```

This will tell the OpenVPN server to validate the username/password entered by clients using the login PAM module. Useful if you have centralized authentication with e.g. Kerberos.

```
plugin /usr/lib/openvpn/openvpn-auth-pam.so login
```

Please read the OpenVPN *hardening security guide*[1] for further security advice.

1.6.2. Configurazione avanzata della rete privata virtuale (bridged VPN) sul server

OpenVPN can be setup for either a routed or a bridged VPN mode. Sometimes this is also referred to as OSI layer-2 versus layer-3 VPN. In a bridged VPN all layer-2 frames - e.g. all ethernet frames - are sent to the VPN partners and in a routed VPN only layer-3 packets are sent to VPN partners. In bridged mode all traffic including traffic which was traditionally LAN-local like local network broadcasts, DHCP requests, ARP requests etc. are sent to VPN partners whereas in routed mode this would be filtered.

1.6.2.1. Preparare la configurazione dell'interfaccia per il collegamento a ponte nel server

Controllare di avere installato il pacchetto bridge-utils:

```
sudo apt-get install bridge-utils
```

Before you setup OpenVPN in bridged mode you need to change your interface configuration. Let's assume your server has an interface eth0 connected to the internet and an interface eth1 connected to the LAN you want to bridge. Your /etc/network/interfaces would like this:

```
auto eth0
iface eth0 inet static
  address 1.2.3.4
  netmask 255.255.255.248
  default 1.2.3.1
```

[1] http://openvpn.net/index.php/open-source/documentation/howto.html#security

```
auto eth1
iface eth1 inet static
  address 10.0.0.4
  netmask 255.255.255.0
```

This straight forward interface config needs to be changed into a bridged mode like where the config of interface eth1 moves to the new br0 interface. Plus we configure that br0 should bridge interface eth1. We also need to make sure that interface eth1 is always in promiscuous mode - this tells the interface to forward all ethernet frames to the IP stack.

```
auto eth0
iface eth0 inet static
  address 1.2.3.4
  netmask 255.255.255.248
  default 1.2.3.1

auto eth1
iface eth1 inet manual
  up ip link set $IFACE up promisc on

auto br0
iface br0 inet static
  address 10.0.0.4
  netmask 255.255.255.0
  bridge_ports eth1
```

At this point you need to restart networking. Be prepared that this might not work as expected and that you will lose remote connectivity. Make sure you can solve problems having local access.

```
sudo service network restart
```

1.6.2.2. Prepare server config for bridging

Modificare il file `/etc/openvpn/server.conf` cambiando le seguenti opzioni:

```
;dev tun
dev tap
up "/etc/openvpn/up.sh br0 eth1"
;server 10.8.0.0 255.255.255.0
server-bridge 10.0.0.4 255.255.255.0 10.0.0.128 10.0.0.254
```

Next, create a helper script to add the *tap* interface to the bridge and to ensure that eth1 is promiscuous mode. Create `/etc/openvpn/up.sh`:

```
#!/bin/sh

BR=$1
ETHDEV=$2
```

```
TAPDEV=$3

/sbin/ip link set "$TAPDEV" up
/sbin/ip link set "$ETHDEV" promisc on
/sbin/brctl addif $BR $TAPDEV
```

Then make it executable:

```
sudo chmod 755 /etc/openvpn/up.sh
```

Una volta configurato il server, riavviare openvpn digitando:

```
sudo service openvpn restart
```

1.6.2.3. Configurazione del client

Installare openvpn sul client:

```
sudo apt-get install openvpn
```

Configurato il server e copiati i certificati del client nella directory `/etc/openvpn/`, creare un file di configurazione per il client copiando l'esempio. Nel computer client, da un terminale, digitare:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn
```

Ora modificare `/etc/openvpn/client.conf` sistemando le seguenti opzioni:

```
dev tap
;dev tun
```

Infine, riavviare openvpn:

```
sudo service openvpn restart
```

Ora dovrebbe essere possibile connettersi alla rete LAN remota attraverso VPN.

1.7. Implementazioni software per client

1.7.1. Linux Network-Manager GUI per OpenVPN

Many Linux distributions including Ubuntu desktop variants come with Network Manager, a nice GUI to configure your network settings. It also can manage your VPN connections. Make sure you have package network-manager-openvpn installed. Here you see that the installation installs all other required packages as well:

```
root@client:~# apt-get install network-manager-openvpn
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  liblzo2-2 libpkcs11-helper1 network-manager-openvpn-gnome openvpn
Suggested packages:
  resolvconf
The following NEW packages will be installed:
  liblzo2-2 libpkcs11-helper1 network-manager-openvpn
  network-manager-openvpn-gnome openvpn
0 upgraded, 5 newly installed, 0 to remove and 631 not upgraded.
Need to get 700 kB of archives.
After this operation, 3,031 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

To inform network-manager about the new installed packages you will have to restart it:

```
root@client:~# restart network-manager
network-manager start/running, process 3078
```

Open the Network Manager GUI, select the VPN tab and then the 'Add' button. Select OpenVPN as the VPN type in the opening requester and press 'Create'. In the next window add the OpenVPN's server name as the 'Gateway', set 'Type' to 'Certificates (TLS)', point 'User Certificate' to your user certificate, 'CA Certificate' to your CA certificate and 'Private Key' to your private key file. Use the advanced button to enable compression or other special settings you set on the server. Now try to establish your VPN.

1.7.2. OpenVPN with GUI for Mac OS X: Tunnelblick

Tunnelblick is an excellent free, open source implementation of a GUI for OpenVPN for OS X. The project's homepage is at *http://code.google.com/p/tunnelblick/*. Download the latest OS X installer from there and install it. Then put your client.ovpn config file together with the certificates and keys in /Users/username/Library/Application Support/Tunnelblick/Configurations/ and lauch Tunnelblick from your Application folder.

```
# sample client.ovpn for Tunnelblick
client
remote blue.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-nocache
auth-retry interact
comp-lzo yes
verb 3
```

```
ca ca.crt
cert client.crt
key client.key
```

1.7.3. OpenVPN with GUI for Win 7

First download and install the latest *OpenVPN Windows Installer*[2]. OpenVPN 2.2.1 was the latest when this was written. Additionally download an alternative Open VPN Windows GUI. The OpenVPN MI GUI from *http://openvpn-mi-gui.inside-security.de* seems to be a nice one for Windows 7. Download the latest version. 20110624 was the latest version when this was written.

You need to start the OpenVPN service. Goto Start > Computer > Manage > Services and Applications > Services. Find the OpenVPN service and start it. Set it's startup type to automatic. When you start the OpenVPN MI GUI the first time you need to run it as an administrator. You have to right click on it and you will see that option.

You will have to write your OpenVPN config in a textfile and place it in C:\Program Files\OpenVPN \config\client.ovpn along with the CA certificate. You could put the user certificate in the user's home directory like in the follwing example.

```
# C:\Program Files\OpenVPN\config\client.ovpn
client
remote server.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-retry interact
comp-lzo yes
verb 3
ca ca.crt
cert "C:\\Users\\username\\My Documents\\openvpn\\client.crt"
key "C:\\Users\\username\\My Documents\\openvpn\\client.key"
management 127.0.0.1 1194
management-hold
management-query-passwords
auth-retry interact
```

1.7.4. OpenVPN per OpenWRT

OpenWRT is described as a Linux distribution for embedded devices like WLAN router. There are certain types of WLAN routers who can be flashed to run OpenWRT. Depending on the available memory on your OpenWRT router you can run software like OpenVPN and you could for example build a small inexpensive branch office router with VPN connectivity to the central office. More

[2] http://www.openvpn.net/index.php/open-source/downloads.html

info on OpenVPN on OpenWRT is *here*[3]. And here is the OpenWRT project's homepage: *http://openwrt.org*

Log into your OpenWRT router and install OpenVPN:

```
opkg update
opkg install openvpn
```

Check out /etc/config/openvpn and put your client config in there. Copy certificated and keys to /etc/openvpn/

```
config openvpn client1
        option enable 1
        option client 1
# option dev tap
        option dev tun
        option proto udp
        option ca /etc/openvpn/ca.crt
        option cert /etc/openvpn/client.crt
        option key /etc/openvpn/client.key
        option comp_lzo 1
```

Restart OpenVPN:

```
service openvpn restart
```

You will have to see if you need to adjust your router's routing and firewall rules.

1.8. Riferimenti

- Per maggiori informazioni, consultare il sito web di *OpenVPN*[4].
- *OpenVPN hardening security guide*[5]
- Un'ottima risorsa è anche *OpenVPN: Building and Integrating Virtual Private Networks*[6] di Pakt (in inglese).

[3] http://wiki.openwrt.org/doc/howto/vpn.overview
[4] http://openvpn.net/
[5] http://openvpn.net/index.php/open-source/documentation/howto.html#security
[6] http://www.packtpub.com/openvpn/book

Capitolo 23. Altre utili applicazioni

Esistono molte applicazioni sviluppate dallo Ubuntu Server Team e altre integrate all'interno della Ubuntu Server Edition che non sono molto conosciute. Questo capitolo presenta alcune di queste utili applicazioni che possono rendere l'amministrazione di un server Ubuntu, o di molti server, più facile.

1. pam_motd

Quando si esegue l'accesso con una versione server di Ubuntu, è possibile vedere dei messaggi giornalieri di informazioni (MOTD). Queste informazioni sono ricavate e visualizzate utilizzando diversi pacchetti:

- *landscape-common*: fornisce le librerie principali di landscape-client, che può essere utilizzato per la gestione di sistemi attraverso l'interfaccia web di *Landscape*. Il pacchetto comprende l'utilità /usr/bin/landscape-sysinfo che può essere usata per recuperare informazioni visualizzate attraverso il MOTD.
- *update-notifier-common:* è usato per aggiornare automaticamente il MOTD per mezzo del modulo pam_motd.

pam_motd esegue gli script in `/etc/update-motd.d` con un ordine basato sul numero anteposto allo script. L'output degli script è memorizzato in `/var/run/motd`, mantenendo l'ordine numerico, quindi concatenato con `/etc/motd.tail`.

È possibile aggiungere delle informazioni dinamiche per il messaggio giornaliero. Per esempio, per aggiungere informazioni meteo locali:

- Installare il pacchetto weather-util:

  ```
  sudo apt-get install weather-util
  ```

- L'utilità weather utilizza i dati METAR dalla «National Oceanic and Atmospheric Administration» e le previsioni meteo dal «National Weather Service». Per reperire informazioni locali è necessario il codice a 4 cifre ICAO. Per ottenere questo codice è possibile consultare il sito web del *National Weather Service*[1].

  Benché il «National Weather Service» sia un'agenzia governativa degli Stati Uniti d'America, stazioni meteo sono disponibili in tutti il mondo. Informazioni meteorologiche potrebbero però non essere disponibili per tutte le località al di fuori del territorio americano.

- Creare il file `/usr/local/bin/local-weather`, un semplice script per usare weather con il proprio indicatore ICAO locale:

  ```
  #!/bin/sh
  #
  #
  # Prints the local weather information for the MOTD.
  #
  #

  # Replace KINT with your local weather station.
  # Local stations can be found here: http://www.weather.gov/tg/siteloc.shtml
  ```

[1] http://www.weather.gov/tg/siteloc.shtml

```
echo
weather -i KINT
echo
```

- Rendere lo script eseguibile:

```
sudo chmod 755 /usr/local/bin/local-weather
```

- Quindi, creare un collegamento simbolico a `/etc/update-motd.d/98-local-weather`:

```
sudo ln -s /usr/local/bin/local-weather /etc/update-motd.d/98-local-weather
```

- Infine, uscire dal server ed effettuare nuovamente l'accesso per visualizzare il nuovo MOTD.

Ora dovrebbe essere possibile visualizzare alcune informazioni utili e delle informazioni riguardo le condizioni meteo locali non del tutto utili. In ogni caso, l'esempio local-weather è utile per dimostrare la flessibilità di pam_motd.

2. etckeeper

etckeeper consente di archiviare il contenuto della directory `/etc` in un sistema di controllo della versione e si integra con apt per inviare le modifiche apportate a `/etc` quando vengono installati o aggiornati pacchetti. Utilizzare un sistema di controllo della versione per gestire la directory `/etc` è considerata una «best practice» e l'obiettivo di etckeeper è quello di rendere questo processo il più facile possibile.

Installare etckeeper digitando quanto segue in un terminale:

```
sudo apt-get install etckeeper
```

Il file di configurazione principale, `/etc/etckeeper/etckeeper.conf`, è molto semplice. L'opzione principale è quale VCS usare. Come impostazione predefinita, etckeeper utilizza bzr per il controllo della versione. Il repository viene automaticamente inizializzato (e viene eseguito il primo commit) durante l'installazione del pacchetto. È possibile annullare questo inserendo il seguente comando:

```
sudo etckeeper uninit
```

Il programma etckeeper esegue i commint delle modifiche a /etc giornalmente.
Questo comportamento può essere disabilitato usando l'opzione di configurazione AVOID_DAILY_AUTOCOMMITS. Inoltre, esegue i commit delle modifiche prima di ogni installazione di un pacchetto. Per un tracciamento delle modifiche più preciso, è consigliato eseguire i commit manualmente aggiungendovi anche un messaggio di commit:

```
sudo etckeeper commit "..Commento sulle modifiche.."
```

Utilizzando i comandi del sistema di controllo è possibile visualizzare il registro delle informazioni riguardo i file in `/etc`:

```
sudo bzr log /etc/passwd
```

Per una dimostrazione dell'integrazione col sistema di gestione dei pacchetti, installare postfix:

```
sudo apt-get install postfix
```

Completata l'installazione, tutti i file di configurazione di postfix dovrebbero essere inviati al repository:

```
Committing to: /etc/
added aliases.db
modified group
modified group-
modified gshadow
```

```
modified gshadow-
modified passwd
modified passwd-
added postfix
added resolvconf
added rsyslog.d
modified shadow
modified shadow-
added init.d/postfix
added network/if-down.d/postfix
added network/if-up.d/postfix
added postfix/dynamicmaps.cf
added postfix/main.cf
added postfix/master.cf
added postfix/post-install
added postfix/postfix-files
added postfix/postfix-script
added postfix/sasl
added ppp/ip-down.d
added ppp/ip-down.d/postfix
added ppp/ip-up.d/postfix
added rc0.d/K20postfix
added rc1.d/K20postfix
added rc2.d/S20postfix
added rc3.d/S20postfix
added rc4.d/S20postfix
added rc5.d/S20postfix
added rc6.d/K20postfix
added resolvconf/update-libc.d
added resolvconf/update-libc.d/postfix
added rsyslog.d/postfix.conf
added ufw/applications.d/postfix
Committed revision 2.
```

Per un esempio di come etckeeper tiene traccia delle modifiche manuali, aggiungere un nuovo host in `/etc/hosts`. Usando bzr è possibile visualizzare quali file sono stati modificati:

```
sudo bzr status /etc/
modified:
  hosts
```

Ora inviare le modifiche:

```
sudo etckeeper commit "nuovo host"
```

Per maggiori informazioni su bzr consultare *Sezione 1, «Bazaar» [268]*.

3. Byobu

Una delle più utili applicazioni per gli amministratori di sistema è screen, che consente l'esecuzione di molteplici shell all'interno di un terminale. Per rendere più semplici alcune delle più avanzate funzionalità di screen e per fornire alcune utili informazioni riguardo il sistema, è stato creato il pacchetto byobu.

Quando byobu è in esecuzione, premendo il tasto *F9* si avrà accesso al menù Configurazione, che consente di:

- Visualizzare il menù dell'aiuto
- Cambiare il colore dello sfondo
- Cambiare il colore di primo piano
- Abilitare notifiche di stato
- Modificare le associazioni dei tasti
- Modificare la sequenza di escape
- Creare nuove finestre
- Gestire le finestre predefinite
- Byobu attualmente non si avvia all'accesso (abilitare)

Le *associazioni di tasti* determinano aspetti come la sequenza di escape, l'apertura di nuove finestre, la modifica delle finestre, ecc... Sono disponibili due insiemi di associazioni di tasti fra cui scegliere: *tasti funzione* e *screen-escape-keys*. Per utilizzare le associazioni predefinite, scegliere *nessuno*.

Byobu fornisce un menù che visualizza la versione del rilascio di Ubuntu, informazioni sul processore, sulla memoria oltre all'ora e alla data, l'effetto è simile a un menù della scrivania.

Utilizzando l'opzione *«Byobu attualmente non si avvia all'accesso (abilitare)»*, byobu sarà lanciato ogni volta che viene aperto un terminale. Le modifiche effettuate su byobu sono relative al singolo utente e non influenzeranno gli altri utenti.

Uno delle differenze nell'uso di byobu è la modalità *scrollback*, alla quale si accede premendo il tasto *F7*. Questa modalità consente di esplorare l'output passato sul terminale utilizzando comandi simili a *vi*. Di seguito vengono riportati alcuni di questi comandi:

- *h*: sposta il cursore a sinistra di un carattere
- *j*: sposta il cursore in giù di una riga
- *k*: sposta il cursore in su di una riga
- *l*: sposta il cursore a destra di un carattere
- *0*: va all'inizio della riga attuale
- *$*: va alla fine della riga attuale
- *G*: va alla riga specificata (come valore predefinito va alla fine del buffer)

- */*: cerca in avanti
- *?*: cerca all'indietro
- *n*: si sposta alla corrispondenza successiva, in avanti o all'indietro

4. Riferimenti

- See the *update-motd man page*[2] for more options available to update-motd.
- L'articolo di «The Debian Package of the Day» riguardo *weather*[3], presenta molte altre informazioni.
- Per maggiori informazioni riguardo l'uso di etckeeper, consultare il *sito web di etckeeper*[4].
- La pagina della *documentazione della comunità su etckeeper*[5].
- Per maggiori informazioni riguardo bzr, consultare il *sito web di bzr*[6].
- Per maggiori informazioni riguardo screen, consultare il *sito web di screen*[7].
- E la pagina della *documentazione della comunità su screen*[8].
- Per maggiori informazioni, consultare anche la *project page*[9] di byobu.

[2] http://manpages.ubuntu.com/manpages/quantal/en/man1/update-motd.1.html
[3] http://debaday.debian.net/2007/10/04/weather-check-weather-conditions-and-forecasts-on-the-command-line/
[4] http://kitenet.net/~joey/code/etckeeper/
[5] https://help.ubuntu.com/community/etckeeper
[6] http://bazaar-vcs.org/
[7] http://www.gnu.org/software/screen/
[8] https://help.ubuntu.com/community/Screen
[9] https://launchpad.net/byobu

Appendice A. Appendice

1. Segnalare bug in Ubuntu Server Edition

Nonostante Il Progetto Ubuntu cerchi di rilasciare software con il minor numero di bug possibile, questi si verificano. È possibile aiutare a correggere questi bug segnalando al progetto quelli che vengono trovati. Il Progetto Ubuntu utilizza *Launchpad*[1] per seguire le segnalazioni di bug; per segnalare un bug relativo a Ubuntu Server su Launchpad, è necessario *creare un account*[2].

1.1. Segnalare bug con ubuntu-bug

Il modo preferito per segnalare un bug è il comando ubuntu-bug; lo strumento ubuntu-bug raccoglie le informazioni sul sistema utili agli sviluppatori per diagnosticare il problema segnalato, che verranno incluse nella segnalazione di bug registrata su Launchpad. Le segnalazioni di bug in ambiente Ubuntu devono essere registrate in relazione a uno specifico pacchetto software e pertanto è necessario inserire in ubuntu-bug il nome del pacchetto in cui si è verificato il bug:

```
ubuntu-bug NOME_DEL_PACCHETTO
```

Per esempio, per registrare un bug relativo al pacchetto openssh-server, è necessario digitare:

```
ubuntu-bug openssh-server
```

In ubuntu-bug è possibile specificare sia un pacchetto binario che un pacchetto sorgente. Usando nuovamente come esempio openssh-server, è inoltre possibile generare un rapporto relativo a openssh, pacchetto sorgente di openssh-server:

```
ubuntu-bug openssh
```

Per ulteriori informazioni sui pacchetti in Ubuntu, consultare *Capitolo 3, Gestione dei pacchetti [21]*.

Il comando ubuntu-bug raccoglie informazioni sul sistema in questione, comprendendo possibilmente informazioni specifiche sullo specifico pacchetto e chiede cosa fare con il materiale raccolto:

```
ubuntu-bug postgresql

*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.
..........

*** Send problem report to the developers?
```

[1] https://launchpad.net/
[2] https://help.launchpad.net/YourAccount/NewAccount

```
After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (1.7 KiB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  C: Cancel
Please choose (S/V/K/C):
```

Le opzioni disponibili sono:

- **Send Report**: selezionando questa opzione le informazioni raccolte vengono inviate a Launchpad come facenti parte del processo di segnalazione di un bug. Si ha l'opportunità di descrivere la situazione che ha condotto al verificarsi del bug.

  ```
  *** Uploading problem information

  The collected information is being sent to the bug tracking system.
  This might take a few minutes.
  91%

  *** To continue, you must visit the following URL:

  https://bugs.launchpad.net/ubuntu/+source/postgresql-8.4/+filebug/kc6eSnTLnLxF8u0t3e56EukFeqJ?

  You can launch a browser now, or copy this URL into a browser on another
  computer.

  Choices:
    1: Launch a browser now
    C: Cancel
  Please choose (1/C):
  ```

  Se si sceglie di avviare un browser, per impostazione predefinita verrà utilizzato il browser web testuale w3m per completare la segnalazione del bug. In alternativa, è possibile copiare l'indirizzo URL in un browser web in esecuzione.

- **View Report**: selezionando questa opzione consente la visualizzazione delle informazioni raccolte in un terminale per un controllo.

  ```
  Package: postgresql 8.4.2-2
  PackageArchitecture: all
  Tags: lucid
  ProblemType: Bug
  ProcEnviron:
    LANG=en_US.UTF-8
    SHELL=/bin/bash
  Uname: Linux 2.6.32-16-server x86_64
  Dependencies:
  ```

```
  adduser 3.112ubuntu1
  base-files 5.0.0ubuntu10
  base-passwd 3.5.22
  coreutils 7.4-2ubuntu2
...
```

Dopo aver visualizzato il rapporto, è possibile ritornare al menù precedente che richiede come procedere.

- **Keep Report File**: selezionando questa opzione, le informazioni raccolte vengono registrate in un file. Questo può essere quindi usato successivamente per una segnalazione di bug o per essere utilizzato in un diverso metodo di segnalazione di Ubuntu. Per inviare il file, inserirlo semplicemente come argomento nel comando ubuntu-bug:

```
What would you like to do? Your options are:
  S: Send report (1.7 KiB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  C: Cancel
Please choose (S/V/K/C): k
Problem report file: /tmp/apport.postgresql.v4MQas.apport

ubuntu-bug /tmp/apport.postgresql.v4MQas.apport

*** Send problem report to the developers?
...
```

- **Cancel**: selezionando questa opzione le informazioni raccolte vengono eliminate.

1.2. Segnalare crash di applicazioni

Il pacchetto software che fornisce l'utilità ubuntu-bug, apport, può essere configurato per essere innescato quando si verifica un crash di un'applicazione. Per impostazione predefinita, è normalmente disabilitato, in quanto il processo di acquisizione di un crash può comportare un importante assorbimento di risorse, in relazione alla quantità di memoria utilizzata dall'applicazione interessata dal crash, quando apport acquisisce ed elabora il core dump.

La configurazione di apport per acquisire informazioni relative al crash di applicazioni richiede un paio di passi. Per prima cosa, è necessario installare gdb, che non è installato in maniera predefinita in Ubuntu Server Edition.

```
sudo apt-get install gdb
```

Per maggiori informazioni sulla gestione di pacchetti in Ubuntu, consultare *Capitolo 3, Gestione dei pacchetti [21]*.

Una volta che gdb è stato installato, aprire il file `/etc/default/apport` con un editor di testo e modificare l'impostazione *enabled* in **1**:

```
# set this to 0 to disable apport, or to 1 to enable it
# you can temporarily override this with
# sudo service apport start force_start=1
enabled=1

# set maximum core dump file size (default: 209715200 bytes == 200 MB)
maxsize=209715200
```

Dopo aver completato la modifica di `/etc/default/apport`, avviare il servizio apport:

```
sudo start apport
```

Dopo il crash di un'applicazione, usare il comando apport-cli per cercare il rapporto salvato con le informazioni sul crash.

```
apport-cli

*** dash closed unexpectedly on 2010-03-11 at 21:40:59.

If you were not doing anything confidential (entering passwords or other
private information), you can help to improve the application by
reporting
the problem.

What would you like to do? Your options are:
  R: Report Problem...
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (R/I/C):
```

Selezionando *Report Problem*, verrà seguito un procedimento simile a quello usato in ubuntu-bug; una importante differenza risiede nel fatto che il rapporto sul crash, quando viene inviato a Launchpad, viene contrassegnato come «privato»: sarà cioé visibile solo a un determinato gruppo di persone, che revisionano i dati così raccolti prima di estendere la visibilità della segnalazione a tutti.

1.3. Risorse

- Consultare la pagina della documentazione della comunità *Reporting Bugs*[3]
- Anche la pagina di *Apport*[4] contiene alcune utili informazioni, sebbene alcune di queste riguardino l'impiego di un'interfaccia grafica.

[3] https://help.ubuntu.com/community/ReportingBugs
[4] https://wiki.ubuntu.com/Apport